ExtremeWare Installation and Release Notes

Software Version 7.4.3b5

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
http://www.extremenetworks.com

Published: December 2005
Part Number: 120300-00 Rev 02

Author: Susan Lynott

Editor:

Production: Susan Lynott

Special Thanks: Abhay

Contents

Chapter 1 Overview

Chapter 4 Clarifications, Known Behaviors, and Resolved Issues

1 Overview

These Release Notes document ExtremeWare®7.4.3b5. ExtremeWare 7.4 enables new hardware products and software features.

NOTE

You can only load ExtremeWare 7.0 (or later) on a switch running ExtremeWare 6.2.2 (or later). To install ExtremeWare 7.4, see "Upgrading ExtremeWare "i" Series Switches" on page 34.

This chapter contains the following sections:

New and Enhanced Features in ExtremeWare 7.4

The following features are introduced or enhanced in ExtremeWare 7.4. These features are documented in detail in the *ExtremeWare 7.4 User Guide* or the *ExtremeWare 7.4 Command Reference Guide*, unless otherwise noted.

Beginning with ExtremeWare 7.4, on bootup and login, switches will display Extreme patent information in the login and bootup banner.

Stacking

Stacking allows users to physically connect up to eight individual Summit® switches together as a single logical unit. This logical unit behaves as a single switch with a single IP address and a single point of authentication.

The stack is controlled by a master switch. There can only be one *stack master* in a stack of switches. The remaining switches in the stack are considered to be *stack members*.

NOTE

Vista support for stacking is not available.

HTTPS/SSL for Network Login

HTTPS access is provided through Secure Socket Layer (SSLv3) and Transport Layer Security (TLS1.0). These protocols enable clients to verify the authenticity of the server to which they are connecting, thereby ensuring that users are not compromised by intruders. SSL supports encryption of the data exchanged between the server and the client, protecting the network login credentials from exposure on the network media.

Source IP Address Protection

Another type of IP address security is automatically placing source IP address filters on all ports. This feature, called source IP lockdown, allows only traffic from a valid DHCP-assigned address or an authenticated static IP address to enter the network. In this way, the network is protected from attacks that use random source addresses for their traffic. When source IP lockdown is enabled, end systems that have a DHCP address or a statically configured IP address can access the network, but all data traffic from a manually configured source IP lockdown is dropped at the switch.

Source IP lockdown is linked to the “disable ARP learning” feature. The same database created when you disable ARP learning is also used by the source IP lockdown feature to create a ACLs that permit traffic from DHCP clients or from statically configured IP ARP entries. All other traffic is dropped.

Summit 400 Link Fault Signaling

Link Fault Signaling is a function of the 10 Gigabit Ethernet port that is defined in the Reconciliation Sublayer, which is implemented on the MAC chip. The local PHY transmits fault messages up to the Reconciliation Sublayer. If the fault is a local fault, the link is brought down locally and a remote fault is automatically sent to the link partner by the MAC. If the fault is a remote fault, the link is marked as being down for the port. All upper layers are notified of the link down state. When a link is marked as up, all upper layers are notified once the remote fault is corrected.

The 10 Gigabit Ethernet link is polled every 100 milliseconds (ms) for link on the Summit 400 switch. When the link is queried, the remote fault is also queried. Link down is indicated to the upper layers if there is a local fault, remote fault, or a true loss of link. Link up is indicated to the upper layers if the fault is removed or link up is determined. In the event that LFS is disabled for remote fault or local fault, a fault will not bring down the link.

EAPS Spatial Reuse

The EAPSv2 spatial reuse feature allows you to configure multiple EAPS domains on the same physical ring. This configuration allows you to use unused ring bandwidth when the ring is complete. When there is only one EAPS domain on the ring, in the complete state, the LAN segment connecting the secondary port of the master switch to the transit switch remains unused. In the complete state, the master keeps its secondary port blocked.

To use the unused LAN segment in a ring complete situation, you can configure multiple EAPS domains on the same physical ring. Each of the protected VLANs belongs to only one of the EAPS

domains in a spatial reuse configuration. By doing this, the entire bandwidth for the ring can be used, including the LAN segment connected to the secondary port of the master switch.

Multicast Extensions

- **Multicast Copy Count**

  Multicast copy count extension allows you to enable or disable this feature using the CLI when you need to configure a copy count of more than 512.

- **Multicast Queue Management**

  Multicast queue management provides a CLI configuration to specify which queues are used for round-robin based load balancing of multicast traffic. It also helps to reduce buffer overflow conditions.

  Using the existing QoS profile configuration, you can set the priority of the queues selected for load balancing. For best system performance, it is advisable to use the same priority to set all the queues being used.

RADIUS Attributes Support for Tunnel Attributes

The following RADIUS attributes are supported in ExtremeWare 7.4. These attributes are included in RADIUS accounting start and stop packets.

- Tunnel-type—VLAN (13)
- Tunnel-medium-type—802
- Tunnel-Private-Group-ID—VLANID

The RADIUS server sends these attributes to the switch to communicate the destination VLAN of the user in the RADIUS Accept message.

When a RADIUS Accept packet is received, the attributes of the packet are parsed and Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID attributes are stored.

Tunnel-Private-Group-ID carries the VLAN ID in a string format. Using the VLAN ID, the VLAN name is derived and used to identify the destination VLAN of the user.

The value for Tunnel-Type must be 13. The value for Tunnel-Medium-type must be 6 for 802 type networks. Tunnel-Private-Group-ID is used for the destination VLAN of a supplicant only when Tunnel-Type and Tunnel-Medium-Type match the values stated above.

Entity MIB

The entity physical table of the entity MIB represents various physical entities present in a device. Some entities are classified as Field Replaceable Units (FRUs). Currently, the odometer feature is available for these FRU entities in the CLI. A private MIB module, EXTREME-ENTITY-MIB, is used to implement the odometer feature.

NOTE

The power supply units are not part of the entity MIB at this time. When the PSUs are added to the ENTITY-MIB, the corresponding odometer value (if any) is added to the extremeEntityFRUTable.

IP ARP Proxy Command Feature

The `configure iparp add proxy` command now configures the `always` qualifier independent of the MAC address configuration. Configuring the IP ARP proxy entry without a mac_address and adding `always` as a qualifier prompts the switch to send the ARP response with the mac_address of the switch. The switch also answers all the ARP requests without filtering requests that belong to the same subnet of the receiving router interface. You can configure up to 64 proxy ARP entries.

```
configure iparp add proxy <ip address> {<mask>} {<mac_address>} {always}
```

Local Authentication for Management Access When RADIUS Server is Enabled

ExtremeWare 7.4 supports local authentication for management sessions if either RADIUS or TACACs is enabled and the servers are configured. Currently, local authentication is performed:

- If both RADIUS/TACACs are disabled
- No RADIUS/TACACs servers are configured
- RADIUS/TACACs servers are not responding

With this new feature, you have the ability to perform local authentication for management sessions while continuing to use RADIUS authentication for Network Login sessions.

Mirroring for Untagged Ports on Summit 200/300/400 Platforms

In the current implementation of ExtremeWare, all packets sent to a mirrored-to port contain a VLAN tag. When looking at the packets, it was easy to see which VLAN the packet was sent on. In ExtremeWare 7.4, packets sent to a mirrored-to port no longer contain a VLAN tag. The mirrored-to port looks like a port in a VLAN. The port is now added as an untagged port if requested by the user. When the mirrored-to port is configured as "untagged," all packets received or sent by any of the mirrored ports are sent to the mirrored-to port without the tag.

Link Layer Discovery Protocol

The Link Layer Discovery Protocol (LLDP) is a Layer 2 protocol (IEEE standard 802.1ab) that is used to determine the capabilities of devices such as repeaters, bridges, access points, routers, and wireless stations. The ExtremeWare 7.4 support for LLDP enables devices to advertise their capabilities and media specific configuration information, and to learn the same information from the devices connected to it. The information is represented in Type Length Value (TLV) format for each data item. The 802.1ab specification provides detailed TLV information.

The information distributed using LLDP is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

EAPS Licensing Consolidation for Summit 200/300/400 Switches

This feature allows you to configure multiple EAPS domains in the EAPS edge switch, provided all the domains have the same set of ring ports. This allows the EAPS edge to be configured to participate in EAPS spatial reuse of a ring.

MAC-Based RADIUS Authentication for Network Login

MAC-based RADIUS authentication uses the MAC address of the client for authentication. This feature is useful for devices that cannot function as 802.1x supplicants, such as IP phones. RADIUS is used as the transport protocol for authentication.

The RADIUS server must be populated with the MAC addresses of all clients or with a MAC address and mask. The MAC address in ASCII format without colons is used as the user name in the RADIUS request, with the locally configured password. While sending RADIUS request the switch will send the configured password in all uppercase letters and the same should be configured on the RADIUS server for the corresponding user name. If a password is not configured locally, then the switch will not send any RADIUS request for that particular supplicant. When a new MAC address is detected on a port that is enabled for MAC-based network login, the RADIUS client sends an authentication message (RADIUS access-request) to the RADIUS server for validation. The RADIUS client tries the configured maximum number of retries to validate the supplicant. During the time between the RADIUS access-request sent by the switch and the RADIUS response sent by the RADIUS server, all traffic sent by the supplicant is blocked. Refer to the *ExtremeWare 7.4 User Guide* for more information.

.Bxtr Software Image

Beginning with ExtremeWare 7.3, ExtremeWare is now offered in two software images: .xtr and .Bxtr. The .Bxtr software image is available on all Summit platforms. It does not support the following features:

- UAA (available on Alpine switches only)
- PoE (available on Alpine switches only)
- SSL (HTTPS)

Although the BlackDiamond 6804 and BlackDiamond 6808 switches use the .xtr software image, the BlackDiamond switches do not support UAA and PoE.

To use SMA and SONET, the advanced image (.xtr or Sxtr) must be used (PD3-10674849 and PD3-10693717).

Features Supported in ExtremeWare 7.4.2 and Later

The following features are supported in ExtremeWare 7.4.2 and later:

- Remote Connect

  Remote Connect Discovery and Attachment Switch VLAN Configuration Requirements

  The discovery and attachment switches should have two separate VLANs: one for direct connect, and a second for remote connect.

  — Direct connect VLAN (or wireless management VLAN)

  The wireless management VLAN is only used for direct connect and upgrading the A300. The A300 comes up faster if the subnet does not have DHCP scope configured, or if it is using forced EDP bootup in Option 43 of the DCHP scope associated to the subnet.

  — Do not use the WMV IP address for the discovery entries in DNS or the attachment IP in redirect-db.

Remote Connect VLAN

The IP address of the remote connect (RC) VLAN is used in DNS for discovery entries (extr-remote-connect-1|2, or defined by Option 43) or for the attachment switch redirect-db.

The RC VLAN of the discovery and attachment switches should be visible from the RC VLANs of the edge (or POE) switches. Run the `ping <Disc RC Vlan IP> from <POE RC VLan IP> command` to verify that the switches are visible from the edge switch.

(PD3-46430702)

- 802.11i Authentication (WPA2)
- Dynamic Frequency Selection (DFS)

New Hardware Platforms for Summit 400 Series Switches

The following new hardware platforms are available on the Summit 400 Series switches with ExtremeWare 7.4. Refer to Table 2 for filename and BootROM filename/version information.

- Summit 400-24p PoE
- Summit 400-24t

Supported Hardware

Hardware in the following sections listed in *italics* is new for this release.

ExtremeWare 7.3 (and later) supports "*i*" series and "e" series products.

Table 1 compares the table capacities of the Summit 400-24 and Summit 400-48 switches.

Table 1: Summit 400-24 and Summit 400-48 system capacities

Description	Summit 400-24	Summit 400-48
Layer 2 Table Size (entries)	16,384	16,384
Layer 3 Host Table Size (entries)	2048	4096
Layer 3 Interface Table Size (entries)	128	256
Layer 3 Multicast (IPMC) Table Size (entries)	128	256
Number ACLs per port	64	128

Table 2 lists software filenames for the hardware that requires software.

Table 2: Software for supported hardware

Extreme Hardware	ExtremeWare Filename	BootROM Filename/Version
BlackDiamond 6816	v743b5.Gxtr or v743b5.SGxtr	ngboot8.2.bin/8.2
BlackDiamond 6808	v743b5.xtr or v743b5.Sxtr	ngboot8.2.bin/8.2
BlackDiamond 6804	v743b5.xtr or v743b5.Sxtr	ngboot8.2.bin/8.2
Alpine 3808	v743b5.xtr or v743b5.Sxtr	ngboot8.2.bin/8.2
Alpine 3804	v743b5.xtr or v743b5.Sxtr	ngboot8.2.bin/8.2
Alpine 3802	v743b5.xtr or v743b5.Sxtr/EW-70-4202.mig	ngboot8.2.bin/8.2

Table 2: Software for supported hardware (continued)

Extreme Hardware	ExtremeWare Filename	BootROM Filename/Version
Summit 400-48t	v743b5.Cxtr or v743b5.SCxtr	s400_boot51.bin
Summit 400-24p	*v743b5.Cxtr or v743b5.SCxtr*	*s405_boot51.bin*
Summit 400-24t	*v743b5.Cxtr or v743b5.SCxtr*	*s405_boot51.bin*
Summit 200-24/48 (see note)	v743b5.Fxtr or v743b5.SFxtr	s200_boot51.bin
Summit 300-24	v743b5.Fxtr or v743b5.SFxtr	s200_boot51.bin
Summit 300-48	v743b5.Lxtr or v743b5.SLxtr	s300_bs.1.1.0.b2.bin s300_bl.1.1.0.b2.bin
Summit7i/7iT	v743b5.Bxtr or v743b5.SBxtr	ngboot8.2.bin/8.2
Summit1i/1iT	v743b5.Bxtr or v743b5.SBxtr	ngboot8.2.bin/8.2
Summit5i/5iT/5iLX	v743b5.Bxtr or v743b5.SBxtr	ngboot8.2.bin/8.2
Summit48i	v743b5.Bxtr or v743b5.SBxtr	ngboot8.2.bin/8.2
Summit48si	v743b5.Bxtr or v743b5.SBxtr	ngboot8.2.bin/8.2
ARM module	v743b5.arm	v743b5.nprom/1.18
OC3 PoS module	v743b5.oc3	v743b5.nprom/1.18
OC12 PoS module	v743b5.oc12	v743b5.nprom/1.18
OC3 ATM module	v743b5.atm3	v743b5.nprom/1.18
MPLS module	v743b5.mpls	v743b5.nprom/1.18
T1 module	v743b5.t1	t1boot28.wr/2.8
E1 module	v743b5.e1	e1boot28.wr/2.8
T3 module	v743b5.t3	t3boot28.wr/2.8

NOTE

In addition to the filenames listed in Table 2, v743b5.Wxtr and v743b5.SWxtr are used for upgrading Summit 200 switches from ExtremeWare 7.1e or ExtremeWare 6.2e.2 versions.

NOTE

The BlackDiamond 6816 requires its own ExtremeWare image. The image that runs on other BlackDiamond, Alpine, or stackable switches does not support the BlackDiamond 6816.

NOTE

Systems with 128 MB memory should use the v743b5.Bxtr or v743b5.SBxtr image. To determine how much memory is available, use the `show memory` *command.*

BlackDiamond Component Support

BlackDiamond components supported with ExtremeWare 7.4, and the minimum ExtremeWare version required by the chassis to support each component, include:

Table 3: BlackDiamond component support

BlackDiamond Component	ExtremeWare Required
BlackDiamond 6804	6.2.2b56[1]
BlackDiamond 6808	6.2.2b56[1]
BlackDiamond 6816	6.2.2b56[1]
MSM-3	7.1.1
MSM64i	6.2.2b56[1]
G8Xi	6.1.3
G8Ti	6.1.3
G12SXi	6.1.4
G16X[3]	7.0.1
G24T[3]	7.0.1
F32Fi	6.1.8
F48Ti	6.1.2
F96Ti	6.1.8
WDMi	6.1.5
10GLRi	7.0
10GX3	7.2.0b18
MPLS	7.0
ARM	7.0
P3cMi	7.0
P3cSi	7.0
P12cMi	7.0
P12cSi	7.0
A3cMi	7.0
A3cSi	7.0
DC Power Supply	6.1.5
110 V AC Power Supply	6.1.5
220 V AC Power Supply	6.1.5

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.

NOTE

Do not install mixed versions of the power supplies in the same system. Install power supplies of the same type.

Alpine Component Support

Alpine components supported with ExtremeWare 7.4, and the minimum ExtremeWare version required, include:

Table 4: Alpine component support

Alpine Component	ExtremeWare Required
Alpine 3802	6.2.2b56[1]
Alpine 3804	6.2.2b56[1]
Alpine 3808	6.2.2b56[1]
SMMi	6.2.2b56[1]
GM-4Si/Xi/Ti	6.1.5
GM-16X[3]	7.0.1
GM-16T[3]	7.0.1
FM-32Ti	6.1.5
FM-24MFi	6.1.5
FM-24Ti	6.1.7
FM-24SFi	6.1.7
FM-32Pi	7.2.0b18
GM-WDMi	6.1.8
WM-4T1i	7.0.1
WM-4E1i	7.0.1
WM-1T3i	7.0.1
FM-8Vi	7.0.1
AC Power Supply	6.1
DC Power Supply	6.1.5

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.

Summit Component Support

Summit components supported with ExtremeWare 7.4, and the minimum ExtremeWare version required, include:

Table 5: Summit component support

Summit Component	ExtremeWare Required
Summit1i	6.2.2b56[1]
Summit5i	6.2.2b56[1]
Summit7i	6.2.2b56[1]
Summit7i DC Power Supply	6.2.2b56[1]
Summit48i	6.2.2b56[1]
Summit48si	6.2.2b56[1]

Table 5: Summit component support

Summit Component	ExtremeWare Required
Summit48si DC Power Supply	7.1.1[2]

1. Older switches do not require ExtremeWare 6.2.2b56. To determine the minimum revision required for your switch, see Field Notice 115A, here: http://www.extremenetworks.com/services/documentation/FieldNotices_FN0115-MACAddressSoftwareReqmt.asp.
2. ExtremeWare 6.2.2 recognizes the Summit48si DC power supply, but does not indicate the type of PSU installed, issue a warning if both an AC and a DC PSU are installed in the same chassis, or send an SNMP trap message when the PSU is hot-swapped.

GBIC Support

GBICs supported with ExtremeWare 7.4, and the minimum ExtremeWare version required, include:

Table 6: GBIC support

GBIC	ExtremeWare Required
SX parallel ID	1.0
SX serial ID	2.0
LX parallel ID	1.0
LX serial ID	2.0
ZX	6.2.2
ZX Rev 03	6.2.2
LX70	2.0
LX100	6.1.9
UTP	6.1.9
SX Mini	7.0.1b11
LX Mini	7.0.1b11
ZX Mini	7.0.1b11

The following table describes how each version of ExtremeWare interprets the media type of the installed GBIC, based on either the Vista web interface, or the `show port configuration` command. All versions correctly identify Parallel ID GBIC types; however, some versions do not correctly identify the Serial ID GBIC type because the Serial ID GBICs were introduced after the software was released.

Table 7: ExtremeWare recognition of GBIC type

ExtremeWare Version	SX Parallel ID	LX Parallel ID	SX Serial ID	LX Serial ID	LX70
1.x	SX	LX	Not Supported	Not Supported	Not Supported
2.x	SX	LX	LX	LX	LX
3.x	SX	LX	CX	CX	CX
4.x	SX	LX	SX	LX	LX
6.x	SX	LX	SX	LX	LX70 (6.1.6 and above)

Table 7: ExtremeWare recognition of GBIC type

ExtremeWare Version	SX Parallel ID	LX Parallel ID	SX Serial ID	LX Serial ID	LX70
7.x	SX	LX	SX	LX	LX70

Mini-GBIC Support

Extreme products support the Extreme mini-GBIC only. For reliability and stability reasons, third-party mini-GBICs are not supported at this time.

XENPAK Module Support

XENPAK modules supported with ExtremeWare 7.4, the minimum ExtremeWare version required, and the manufacturers supported include:

Table 8: XENPAK support

XENPAK Module	ExtremeWare Required	Manufacturers Supported
LR	7.2.0b18	Intel, Opnext
ER	7.2.0b18	Intel, Opnext

Channel Mapping

Table 9 lists the channel mapping for Altitude 300-2i wireless ports connected to a Summit 300-48 using ExtremeWare 7.4. The UAA features contained in this table apply to the Summit 300-48 switch only.

Table 9: Altitude 300-2i channel mapping

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Canada	CA	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11
Hong Kong	HK	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11
United States	US	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11
Japan	JP	34/38/42/46	1-13	1-14
Argentina	AR	52/56/60/64/149/153/157/161	1-13	1-13
Australia	AU	36/40/44/48/52/56/60/64/149/153/157/161/165	1-13	1-13
Austria	AT	36/40/44/48	1-13	1-13
Belgium	BE	36/40/44/48/52/56/60/64	1-13	1-13
Brazil	BR	36/40/44/48/149/153/157/161/165	1-13	1-13
Chile	CL	149/153/157/161/165	None	1-13
China	CN	149/153/157/161/165	1-13	1-13
Colombia	CO	36/40/44/46/52/56/60/64/149/153/157/161/165	1-11	1-11
Costa Rica	CR	None	1-13	1-13
Cyprus	CY	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 9: Altitude 300-2i channel mapping (continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Czech Republic	CZ	36/40/44/48/52/56/60/64	1-13	1-13
Denmark	DK	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Egypt	EG	None	1-13	1-13
Estonia	EE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Finland	FI	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
France	FR	36/40/44/48/52/56/60/64	1-13	1-13
Germany	DE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Greece	GR	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Hungary	HU	36/40/44/48	1-13	1-13
Iceland	IS	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
India	IN	None	1-13	1-13
Indonesia	ID	None	1-13	1-13
Ireland	IE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Israel	IL	None	1-13	1-13
Italy	IT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Jordan	JO	36/40/44/48	1-13	1-13
Korea ROC (south)	KR	149/153/157/161	1-13	1-13
Kuwait	KW	None	1-13	1-13
Latvia	LV	None	1-13	1-13
Liechtenstein	LI	36/40/44/48/52/56/60/64	1-13	1-13
Lithuania	LT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Luxembourg	LU	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Malaysia	MY	52/56/60/64/149/153/157/161	1-11	1-11
Mexico	MX	36/40/44/48/52/56/60/64/149/153/157/161	1-11	1-11
Netherlands	NL	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
New Zealand	NZ	36/40/44/48/52/56/60/64/149/153/157/161/165	1-13	1-13
Norway	NO	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Poland	PL	36/40/44/48/52/56/60/64100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Portugal	PT	36/40/44/48/52/56/60/64100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 9: Altitude 300-2i channel mapping (continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Puerto Rico	PR	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11
Russia	RU	None	1-13	1-13
Saudi Arabia	SA	None	1-13	1-13
Singapore	SG	149/153/157/161/165	1-13	1-13
Slovak Republic	SK	36/40/44/48/52/56/60/64	1-13	1-13
Slovenia		36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
South Africa	ZA	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Spain	SP	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Sweden	SE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Switzerland	CH	36/40/44/48/52/56/60/64	1-13	1-13
Taiwan	TW	56/60/64/149/153/157/161	1-11	1-11
Thailand	TH	149/153/157/161	1-13	1-13
Turkey	TR	36/40/44/48/52/56/60/64	1-13	1-13
United Arab Emirates	AE	None	1-13	1-13
United Kingdom	GB	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 10 lists the channel mapping for indoor Altitude 300-2d wireless ports connected to a Summit 300-48 switch using ExtremeWare 7.4.

Table 10: Altitude 300-2d indoor channel mapping

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Canada	CA	52/56/60/64/149/153/157/161/165	1-11	1-11
Hong Kong	HK	52/56/60/64/149/153/157/161/165	1-11	1-11
United States	US	52/56/60/64/149/153/157/161/165	1-11	1-11
Japan	JP	34/38/42/46	1-13	1-14
Argentina	AR	52//56/60/64/149/153/157/161	1-13	1-13
Australia	AU	52/56/60/64/149/153/157/161/165	1-13	1-13
Austria	AT	36/40/44/48	1-13	1-13
Belgium	BE	36/40/44/48/52/56/60/64	1-13	1-13
Brazil	BR	149/153/157/161/165	1-13	1-13
Chile	CL	149/153/157/161/165	1-13	1-13
China	CN	149/153/157/161/165	None	1-13
Colombia	CO	52/56/60/64/149/153/157/161/165	1-11	1-11
Costa Rica	CR	None	1-13	1-13

Table 10: Altitude 300-2d indoor channel mapping (continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Cyprus	CY	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Czech Republic	CZ	36/40/44/48/52/56/60/64	1-13	1-13
Denmark	DK	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Egypt	EG	None	1-13	1-13
Estonia	EE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Finland	FI	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
France	FR	36/40/44/48/52/56/60/64	1-13	1-13
Germany	DE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Greece	GR	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Hungary	HU	36/40/44/48	1-13	1-13
Iceland	IS	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
India	IN	None	1-13	1-13
Indonesia	ID	None	1-13	1-13
Ireland	IE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Israel	IL	None	1-13	1-13
Italy	IT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Jordan	JO	36/40/44/48	1-13	1-13
Korea ROC (south)	KR	149/153/157/161	1-13	1-13
Kuwait	KW	None	1-13	1-13
Latvia	LV	None	1-13	1-13
Liechtenstein	LI	36/40/44/48/52/56/60/64	1-13	1-13
Lithuania	LT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Luxembourg	LU	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Malaysia	MY	52/56/60/64/149/153/157/161	1-11	1-11
Mexico	MX	52/56/60/64/149/153/157/161	1-11	1-11
Netherlands	NL	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
New Zealand	NZ	36/40/44/48/52/56/60/64/149/153/157/161/165	1-13	1-13
Norway	NO	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Poland	PL	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 10: Altitude 300-2d indoor channel mapping (continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Portugal	PT	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Puerto Rico	PR	36/40/44/48/52/56/60/64/149/153/157/161/165	1-11	1-11
Russia	RU	None	1-13	1-13
Saudi Arabia	SA	None	1-13	1-13
Singapore	SG	149/153/157/161/165	1-13	1-13
Slovak Republic	SK	36/40/44/48/52/56/60/64	1-13	1-13
Slovenia		36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
South Africa	ZA	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Spain	SP	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Sweden	SE	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Switzerland	CH	36/40/44/48/52/56/60/64	1-13	1-13
Taiwan	TW	56/60/64/149/153/157/161	1-11	1-11
Thailand	TH	149/153/157/161	1-13	1-13
Turkey	TR	36/40/44/48/52/56/60/64	1-13	1-13
United Arab Emirates	AE	None	1-13	1-13
United Kingdom	GB	36/40/44/48/52/56/60/64/100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 11 lists the channel mapping for outdoor Altitude 300-2d wireless ports connected to a Summit 300-48 switch using ExtremeWare 7.4.

Table 11: Altitude 300-2d outdoor channel mapping

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Canada	CA	52/56/60/64/149/153/157/161/165	1-11	1-11
Hong Kong	HK	52/56/60/64/149/153/157/161/165	1-11	1-11
United States	US	52/56/60/64/149/153/157/161/165	1-11	1-11
Japan	JP	None	1-13	1-14
Argentina	AR	52//56/60/64/149/153/157/161	1-13	1-13
Australia	AU	52/56/60/64/149/153/157/161/165	1-13	1-13
Austria	AT	None	1-13	1-13
Belgium	BE	None	1-13	1-13
Brazil	BR	149/153/157/161/165	1-13	1-13
Chile	CL	149/153/157/161/165	None	1-13
China	CN	149/153/157/161/165	1-13	1-13
Colombia	CO	52/56/60/64/149/153/157/161/165	1-11	1-11

Table 11: Altitude 300-2d outdoor channel mapping (continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Costa Rica	CR	None	1-13	1-13
Cyprus	CY	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Czech Republic	CZ	None	1-13	1-13
Denmark	DK	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Egypt	EG	None	1-13	1-13
Estonia	EE	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Finland	FI	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
France	FR	None	1-7	1-7
Germany	DE	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Greece	GR	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Hungary	HU	None	1-13	1-13
Iceland	IS	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
India	IN	None	1-13	1-13
Indonesia	ID	None	1-13	1-13
Ireland	IE	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Israel	IL	None	5-7	5-7
Italy	IT	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Jordan	JO	None	1-13	1-13
Korea ROC (south)	KR	149/153/157/161	1-13	1-13
Kuwait	KW	None	1-13	1-13
Latvia	LV	None	1-13	1-13
Liechtenstein	LI	None	1-13	1-13
Lithuania	LT	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Luxembourg	LU	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Malaysia	MY	52/56/60/64/149/153/157/161	1-11	1-11
Mexico	MX	52/56/60/64/149/153/157/161	1-11	1-11
Netherlands	NL	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
New Zealand	NZ	52/56/60/64/149/153/157/161/165	1-13	1-13
Norway	NO	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Poland	PL	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Portugal	PT	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Puerto Rico	PR	52/56/60/64/149/153/157/161/165	1-11	1-11
Russia	RU	None	1-13	1-13
Saudi Arabia	SA	None	1-13	1-13
Singapore	SG	149/153/157/161/165	1-13	1-13
Slovak Republic	SK	None	1-13	1-13
Slovenia	SI	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
South Africa	ZA	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Spain	SP	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Table 11: Altitude 300-2d outdoor channel mapping (continued)

Country	Country Code	802.11a Channels	802.11g Channels	802.11b Channels
Sweden	SE	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13
Switzerland	CH	None	1-13	1-13
Taiwan	TW	149/153/157/161	1-11	1-11
Thailand	TH	149/153/157/161	1-13	1-13
Turkey	TR	None	1-13	1-13
United Arab Emirates	AE	None	1-13	1-13
United Kingdom	GB	100/104/108/112/116/120/124/128/132/136/140	1-13	1-13

Tested Third-Party Products

This section lists the third-party products tested for the Summit 300-48 switch. The UAA features contained in this section apply to the Summit 300-48 switch only.

Tested NICs

The wireless NICs in Table 12, Table 13, Table 14, and Table 15 are tested with the listed software (or later) and authentication method.

Table 12: 802.11 a/b/g wireless NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
Proxim A/B/G Gold	2.4.2.1.7 2.3.0.75	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS
NetGear WAG511	2.4.1.130	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS
D-link DWL-AG650 Air-Expert	1.2.0.1	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS PEAP/TLS/TTLS
D-link DWL-AG660 Air Premier	2.1.3.1	WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS
3Com 3CRWE154A72	3.0.0.46	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS
Linksys AG WPC55AG	2.3.2.4	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS PEAP/TLS
Cisco Air-CB21AG	3.0.0.111	W2K SP4 WinXP SP1/SP2	Card Utility	PEAP/TLS

Table 13: 802.11 a/b wireless NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
Linksys WPC51AB	2.0.1.254	W2K SP4 WinXP SP/SP21	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
Orinoco Gold A/B	7.64.1.316	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
D-Link DWL-650 AB Air Pro	2.4.1.130	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS

Table 14: 802.11b wireless NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
Cisco Aironet350 b	8.1.6.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS
Netgear MA401 b-only	2.0.2.0	W2K SP4	Odyssey 2.2/Card Utility	PEAP/TLS PEAP/TLS
Microsoft b card MN520	D-link 2.0.1.254	W2K SP4 WinXP SP1	Odyssey 2.2	PEAP/TLS PEAP/TLS
3Com 11b-only 3CRWE60292B	2.1.1.3005	W2K SP4 WinXP SP1	Odyssey 2.2/Card Utility	PEAP/TLS PEAP/TLS/TTLS

Table 15: 802.11g wireless NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
NetGear WG511	2.1.25.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS
Buffalo WLI-CB-G54	3.50.21.10	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
Linksys WPC54G	3.20.21.0	WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
D-Link DWL G650Airplus	2.2.2.71	W2K SP4 WinXP SP1/SP2	Odyssey 2.23.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
D-Link DWL-G650-B2	2.21.4.71	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS
Microsoft MN-720	3.20.26.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS PEAP/TLS/TTLS

Table 16: 802.11g MiniPCI wireless NIC

NIC	Driver	OS	Third-Party Software	Authentication Method
Broadcom 54G MaxPerformance	3.20.23.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS
Dell True Mobile 1300	3.20.23.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS

The wireless PCI cards in Table 17 are tested with the listed software (or later) and authentication method.

Table 17: Wireless PCI cards

NIC	Driver	OS	Third-Party Software	Authentication Method
Linksys WMP54G	3.30.15.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS
NetGear WAG311 Tri-mode	3.0.0.43	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS
NetGear WG311	2.4.0.71	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS

WPA-Compliant Wireless NICs

The wireless NICs in Table 18, Table 19, and Table 20 are WPA-compliant.

NOTE

WPA compliant wireless NICs support TKIP and AES with pre-shared and dynamic keys.

Table 18: Wireless tri-mode NICs

NIC	Driver	OS	Third-Party Software	Authentication Method
NetGear WAG511	2.4.1.130	W2K SP4 WinXP SP1/SP21	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
D-link DWL-AG650 AirExpert	1.2.0.1	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
3Com 3CRWE154A72	3.0.0.46	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS

Table 18: Wireless tri-mode NICs (continued)

NIC	Driver	OS	Third-Party Software	Authentication Method
3Com 3CRPAG175	1.0.0.25	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Proxim A/B/G	2.4.2.1.7	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.02	PEAP/TLS/TTLS
D-Link AG660	2.1.3.1	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Linksys AG WPC55AG	3.0.0.111	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Cisco Air-CB21AG	3.0.0.111	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS

Table 19: Wireless 802.11g NICs (WPA compliant)

NIC	Driver	OS	Third-Party Software	Authentication Method
Buffalo WLI-CB-G54	3.50.21.10	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
NetGear WG511T	3.3.0.156	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
NetGear WAG511	2.4.1.130	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	WPA-PSK
Linksys WPC54G	3.20.21.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
D-Link DWL-G650-B2	2.2.4.71	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Microsoft MN-720	3.20.21.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS

Table 20: Wireless 802.11 a/b NICs (WPA compliant)

NIC	Driver	OS	Third-Party Software	Authentication Method
D-link AirPro AB650	2.4.1.130	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS

Table 20: Wireless 802.11 a/b NICs (WPA compliant)

NIC	Driver	OS	Third-Party Software	Authentication Method
NetGear WAB501	2.4.0.71	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS
Avaya Platinum A/B	2.4.1.21	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0	PEAP/TLS/TTLS

Table 21: Wireless 802.11 a/b/g PCI-NICs (WPA Compliant)

NIC	Driver	OS	Third-Party Software	Authentication Method
Dell True Mobile 1450	3.40.65.0	W2K SP4 WinXP SP1/SP2	Odyssey 2.2/3.0/4.0 Card Utility	PEAP/TLS/TTLS

Tested RADIUS Servers

These RADIUS servers are fully tested:

- Microsoft Internet Authentication Server
- Funk Steel Belted RADIUS Enterprise Edition 4.5
- Meeting House
- Free Radius
- InfoBlox RadiusONE
- Roving Planet
- Cisco ACS

Tested Third-Party Clients

These third-party clients are fully tested:

- Funk Odyssey 2.2
- MeetingHouse Data AEGIS 2.0.5
- Odyssey 3.00.0.937

Tested Laptops

These laptops are fully tested:

- IBM Thinkpad T40 (Intel Centrino-based 802.11b)
- IBM Thinkpad T41 (Intel Centrino-based 802.11b)
- Dell Latitude D800 (Intel Centrino-based 802.11b)
- HP/Compaq nx9010 (Broadcom 54G MaxPerformance MiniPCI)
- Fujitsu Lifebook N series (Broadcom 54G MaxPerformance MiniPCI)

- Sony PCG-K15
- Dell Latitude D600

Tested PDAs

These PDAs are fully tested:

- iPAQ H5550
- Dell Axim x3i
- HP Pocket PC 4155

Tested Tablets

These tablets are fully tested:

- NEC Tablet

Tested Scanner

The following scanner is fully tested:

- Intermec Scanner Model 700 Color-Pocket PC - 802.11b CF: Open Authentication/No encryption, Shared/WEP, and Open/WEP

Tested Embedded WNIC Modules

- Dell Truemobile 1200, 1300, 1350, 1450
- IBM Thinkpad T40p Trimode (Centrino card)

Tested Spectralink Supported Handsets

- Avaya 3606
- Spectralink Netlink 1640

Tested Spectralink Gateway

- Netlink SVP Avaya Voice Priority Processor
- Netlink SVP100 Gateway

Legacy IP Phones

These wired IP phones have been verified for PoE power up only:

- Avaya 4610SW IP
- Avaya 4620 IP New 03-016A/B
- Avaya 4620SW IP
- Super tex PD1 v1
- Super PD+PS

- TI PTB48540 CL003ENG
- 3COM NJ105
- 3COM NJ220
- 3COM NJ200 Old
- 3COM NJ200 New
- 3COM NJ100 New
- 3COM NJ100 Old
- 3COM 3C10248B with 3CNJVOIPMOD-NBX
- 3COM 3C10248PE IP Phone
- 3COM 3C10226PE IP Phone
- Avaya 4602SW IP Phone
- Avaya 4620 IP Phone
- Avaya 4630SW IP Phone
- Polycom IP 300 With 2457-11077-002 Rev.X1
- Polycom IP 500 With 2457-11077-002 Rev.X1
- Polycom IP 600
- Polycom Speaker IP 3500 with Cisco PIM
- Polycom Speaker IP 3500 with IEEE
- Linear CD671
- 3COM 655003403 PD with 3CNJVOIPMOD-NBX
- Avaya 4602 IP Phone
- Linear LTC4257IS8 with 4257
- Linear Edge PD
- TPS2375 Eval Chip #22
- TPS2375 Eval Chip #20
- Siemens Optipoint 410 Standard FV
- Siemens Optipoint 410 Entry FV
- Polycom SoundPoint IP LAN/Power Cable

Legacy Phones with Dongle

- Cisco 7910
- Cisco 7940
- Cisco 7960
- Cisco 7970

2 Upgrading to ExtremeWare 7.4

This chapter contains the following sections:

Staying Current

If you are an Extreme Assist customer, the latest release and release notes are available after logging in to the Tech Support web site:

http://www.extremenetworks.com/go/esupport.htm.

ExtremeWare Software Images for Summit 200/300/400 Series Switches

Table 22 lists the software images for the ExtremeWare Summit 200/300/400 Series switches and describes the purpose of each image.

Table 22: ExtremeWare 7.4 software images

Filename	Description and Usage
s200_boot51.bin	This is the BootROM file version 5.1 for Summit 200-24, Summit 200-48, and Summit 300-24 Series switches. The Summit 300-24 switch is architecturally the same as the Summit 200-24 except it offers PoE functionality. When upgrading to ExtremeWare 7.4 or later from ExtremeWare 6.2e or ExtremeWare 7.1e, it is likely those switches will have older BootROM versions. The wrapper image (files that end with .Wxtr) will automatically upgrade the BootROM to the required version of 5.1, if necessary.

Table 22: ExtremeWare 7.4 software images

Filename	Description and Usage
s300_bl.1.1.0.b2.bin	This is the BootLoader file version 1.1.0 for the Summit 300-48 (build 2). Generally, most Summit 300-48 switches will be running at least this version. If this is not the case, download the BootLoader as stated in the upgrade steps.
s300_bs.1.1.0.b2.bin	This is the BootStrap file version 1.1.0 for the Summit 300-48 (build 2). Generally, most Summit 300-48 switches will be running at least this version. If this is not the case, download the BootStrap as stated in the upgrade steps.
s400_boot51.bin	This is the BootROM file version 5.1 for the Summit 400-48. When upgrading to ExtremeWare 7.4, ensure that the BootROM in your Summit 400 is at least version 5.1. If this is not the case, follow the upgrade steps to update the BootROM version 5.1.
s405_boot51.bin	This is the BootROM file version 5.1 for the Summit 400-24t and Summit 400-24p.
v743b5.Wxtr	This is the wrapper image for the Summit 200 series switches, also known as the intermediate image. Since ExtremeWare 7.3e is much larger image compared to ExtremeWare 6.2e or 7.1e, this image is needed to repartition the flash to store the ExtremeWare 7.3e image and the configuration. It should be used only when upgrading Summit 200-24, Summit 200-48 switches running version ExtremeWare 6.2e or ExtremeWare 7.1e releases to ExtremeWare 7.4.
v743b5.SWxtr	This is the same as v73e0b43.Wxtr except this file supports SSH functions.
v743b5.Fxtr	This is the actual ExtremeWare 7.4 image for Summit 200-24, Summit 200-48, Summit 300-24 series switches.
v743b5.SFxtr	This is the same as v743b5.Fxtr except this file supports SSH functions.
v743b5.Lxtr	This is the actual ExtremeWare 7.4 image for the Summit 300-48 series switch.
v743b5.SLxtr	This is the same as v743b5.Lxtr except this file supports SSH functions.
v743b5.Cxtr	This is the actual ExtremeWare 7.4 image for the Summit 400-48t, Summit 400-24t, and Summit 400-24p series switch
v743b5.SCxtr	This is the same as v743b5.Cxtr except this file supports SSH functions.
v743b5.mib	This is the MIB file associated with this release.

Upgrading ExtremeWare “i” Series Switches

You can only load ExtremeWare 7.0 (or later) on a switch running ExtremeWare 6.2.2b56 (or later). You can only load ExtremeWare 6.2.2 on a switch running ExtremeWare 6.1.9 (or later). Table 23 lists the BootROM required for each version of ExtremeWare.

Table 23: Required BootROM versions

ExtremeWare Version	BootRom Version
ExtremeWare 7.3 and later	BootROM 8.2 (or later)
ExtremeWare 7.1.1 through ExtremeWare 7.2.0	BootROM 8.1 (or later)
ExtremeWare 7.0.0 through ExtremeWare 7.1.0	BootROM 7.8 (or later)
ExtremeWare 6.2.2 through ExtremeWare 6.2.2	BootROM 7.8
ExtremeWare 6.1.8 through ExtremeWare 6.2.1	BootROM 7.2 (or later)

Table 23: Required BootROM versions

ExtremeWare Version	BootRom Version
ExtremeWare 6.1 through ExtremeWare 6.1.7	BootROM 6.5

If your switch is running ExtremeWare 6.1.8 (or earlier), you must first upgrade to ExtremeWare 6.1.9, then upgrade to ExtremeWare 6.2.2b56 (or later). Following are specific instructions on upgrading to, and downgrading from, ExtremeWare 7.3 for Summit, Alpine, and BlackDiamond switches.

Alpine switches with PoE modules require user intervention using a CLI command to upgrade the PoE firmware. Until the firmware update is completed, the PoE ports are not powered up. Refer to "Upgrading PoE Firmware on an Alpine Switch with a PoE Module" on page 40.

Upgrading Switches to ExtremeWare 7.4

To install ExtremeWare 7.4, you must:

1. Save the configuration to a TFTP server.
2. Upgrading the BootROM to Version 8.2 as described on page 36.
3. Upgrading to ExtremeWare 6.1.9 as described on page 36.
4. Upgrading to ExtremeWare 6.2.2b56 as described on page 37.
5. Upgrading to ExtremeWare 7.4 as described on page 37.
6. Upgrading T1, E1, or T3 Modules from a Release Prior to ExtremeWare 6.1.8b79 as described on page 38.
7. Upgrading T1, E1, or T3 Modules from ExtremeWare 6.1.8b79 or Later as described on page 39.
8. Upgrade ATM, MPLS, ARM, or PoS modules as described on page 39.
9. Upgrade the PoE firmware, if required, on the Alpine switch as described on page 40.

If you have already installed ExtremeWare 6.1.9 through ExtremeWare 6.2.2b43, you can skip step 3. If you have already installed ExtremeWare 6.2.2b56 through ExtremeWare 7.0.1, you can skip steps 3 and 4.

NOTE

If you are also upgrading your BlackDiamond to MSM-3's, see the MSM-3 Upgrade Note *included with your MSM-3.*

NOTE

The Alpine 3802 requires a different upgrade procedure, described on page 40.

Saving the Current Configuration

Before upgrading ExtremeWare, save your configuration using the following steps. This preserves the ability to downgrade should it become necessary.

1. If you are using the Network Login campus mode:
   a. Disable Network Login using the `disable netlogin` command to prevent users from re-authenticating during the backup process.

b Use the `clear netlogin state port` command on all Network Login user ports, causing all Network Login users to be unauthenticated and all client ports to move back to their respective unauthenticated VLAN configuration.

c Use the `show netlogin` and `show vlan` commands to verify that all Network Login ports are in the unauthenticated state and the client ports are members of their respective unauthenticated VLANs.

2 If you are using ACLs and the CPU DoS protect feature, ensure that the CPU DoS protect filter precedence follows the rules described in "CPU DoS Protect and ACL Precedence" on page 62. If there is a precedence conflict, CPU DoS protect is not enabled.

3 Save the current configuration in both the primary and secondary configuration spaces using the `save configuration primary` and `save configuration secondary` commands.

4 Configure the switch to use the primary image and the primary configuration using the `use image primary` and `use configuration primary` commands.

5 Verify that all of the above procedures were completed successfully with the `show switch` command.

6 Upload the configuration to a TFTP server for safekeeping using the `upload configuration` command.

Upgrading the BootROM to Version 8.2

Before you upgrade ExtremeWare, upgrade to BootROM 8.2 (BootROM 8.2 is compatible with all ExtremeWare versions back to ExtremeWare 6.1.9):

1 Download the BootROM using the `download bootrom [<host_name> | <ip_addr>] <ngboot82.bin_name>` command.

2 Reboot the switch using the `reboot` command.

Upgrading to ExtremeWare 6.1.9

If you are running ExtremeWare 6.1.8 (or earlier), upgrade to ExtremeWare 6.1.9:

1 TFTP download ExtremeWare 6.1.9 to the primary image space using the `download image primary` command.

NOTE

If you do not upgrade to ExtremeWare 6.1.9 before downloading ExtremeWare 6.2.2, the ExtremeWare 6.2.2 download will fail, and the following message will be printed from the system:

```
ERROR: File too large
```

2 Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved.

3 Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.

4 Check the log for configuration errors. Manually enter configurations that did not load.

5 If you configured Random Early Drop Probability in ExtremeWare 6.1.8 (or earlier), re-configure the Random Early Drop Probability using the `configure red drop-probability` command.

6 Save the configuration to the primary space.

Upgrading to ExtremeWare 6.2.2b56

If you are running ExtremeWare 6.1.9 to ExtremeWare 6.2.2b43, upgrade to ExtremeWare 6.2.2b56 (you can substitute ExtremeWare 6.2.2 builds 68, 108, 124, 134, and 156 for build 56):

1. TFTP download ExtremeWare 6.2.2b56 to the primary image space using the `download image primary` command.
2. Reboot the switch using the `reboot` command. The previous configuration of the switch is preserved.

   NOTE

   ExtremeWare 6.2.2b56 (and later) stores 75 static log entries. Previous versions stored 100 entries. To accommodate the new entry limit, ExtremeWare 6.2.2b56 clears the static log after your first reboot. To preserve your static log entries, use the `show log` *command and save the output.*

3. Verify that the correct BootROM and ExtremeWare version are loaded using the `show switch` and `show version` commands.
4. TFTP download the saved configuration, and answer `y` at the prompt to reboot the switch.
5. Check the log for configuration errors. Manually enter configurations that did not load.
6. Save the configuration.

   Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

   NOTE

   After upgrading from ExtremeWare 6.1.9 to ExtremeWare 6.2.2, the IGMP snooping leave time-out value will be changed from 10 seconds to 0. This results in an IGMP snooping membership entry being removed immediately when an IGMP leave is received from a host.

   This is good for an environment where only one host is connected. Use the `configure igmp snooping leave-timeout` *command to change the leave time-out value back to 10 seconds.*

Upgrading to ExtremeWare 7.4

If you are running any software image from ExtremeWare 6.2.2b56 or later, upgrade to ExtremeWare 7.4:

NOTE

If you are upgrading a chassis with MSM64i's to MSM-3's, see the MSM-3 Upgrade Note included with your MSM-3.

1. Upload the configuration to your TFTP server using the `upload configuration` command.
2. TFTP download ExtremeWare 7.4 to the primary image space using the `download image primary` command.
3. Clear your switch using the `unconfigure switch all` command, and enter `y` at the prompt to reboot the switch. If you started the upgrade process with ExtremeWare 6.2.2b56 or later, you can skip this step.
4. Configure the IP address on the switch to reach the TFTP server.

5 TFTP download the configuration.

6 Reboot the switch using the `reboot` command.

NOTE

If you have hitless failover enabled on your MSM-3, you can use the hitless upgrade procedure.

7 Verify that the correct ExtremeWare version is loaded on the switch using the `show switch` command.

8 TFTP download the configuration you saved in Step 1, and enter `y` at the prompt to reboot the switch.

NOTE

If you are using EAPS and are upgrading from a version prior to ExtremeWare 6.2.2b134 or from ExtremeWare 7.0, the default failtimer expiry action changes to sending an alert. This keeps your ring from failing over when there is no break in the ring, such as in the event of a broadcast storm, busy CPU, or misconfigured control VLAN. To change the failtimer expiry action to opening the secondary port, especially if your EAPS traffic flows through switches that do not support EAPS, use the configure eaps failtime expiry-action command.

9 Check the log for configuration errors. Manually enter configurations that did not load.

10 Save the new configuration to the primary space.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

11 If you are upgrading a BlackDiamond switch, synchronize the BootROM, image, and configuration across all installed MSM modules using the `synchronize` command. This command reboots the synchronized modules.

You can ignore any diagnostics failure messages generated by the synchronization.

12 Reboot the switch using the `reboot` command.

13 If you are using the Network Login campus mode:

a Manually enable Network Login using the `enable netlogin [web-based | dot1x]` command.

b Verify that users are able to authenticate and successfully access network resources.

Upgrading T1, E1, or T3 Modules from a Release Prior to ExtremeWare 6.1.8b79

If you are using a T1, E1, or T3 module with an ExtremeWare release prior to 6.1.8b79 or a BootROM prior to 2.8, upgrade the module to ExtremeWare 7.3:

1 TFTP download ExtremeWare 6.1.8b79 for the module using the `download image slot primary` command.

NOTE

T1, E1, and T3 modules must be using ExtremeWare 6.1.8b79 and BootROM 2.8 before upgrading to ExtremeWare 7.3.

2 Configure the module to use the primary image with the `use image primary slot` command.

3 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 3 until you have upgraded every module, then reboot the switch instead of rebooting each slot.

4 Verify that the correct ExtremeWare is loaded using the `show version` command. You should see output similar to the following:

```
BootROM: 251.251
Image: WM4T1 Version 6.1.8 (Build 79)
```

If you see a version other than Build 79, repeat steps 1 - 4.

5 Download the BootROM using the `download bootrom slot` command.

6 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 6, upgrade every module, then reboot the switch.

7 Download the latest ExtremeWare to the primary image space.

8 Reboot the module using the `reboot slot` command.

Upgrading T1, E1, or T3 Modules from ExtremeWare 6.1.8b79 or Later

If you are using a T1, E1, or T3 module with ExtremeWare 6.1.8b79 (or later) and BootROM 2.8 (or later), upgrade the module to ExtremeWare 7.4:

1 TFTP download the latest ExtremeWare for the module using the `download image slot primary` command.

2 Configure the module to use the primary image with the `use image primary slot` command.

3 Reboot the module using the `reboot slot` command.

Upgrading ATM, MPLS, ARM, or PoS Modules from a Release Prior to ExtremeWare 7.4

If you are using an ATM, MPLS, ARM, or PoS module with a previous ExtremeWare release or a BootROM prior to 1.18, upgrade the module to ExtremeWare 7.4:

1 Upgrade your switch to ExtremeWare 7.4 by following the upgrade instructions "Upgrading Switches to ExtremeWare 7.4" on page 35. When your switch is successfully booted on ExtremeWare 7.4 continue with step #2.

2 TFTP download ExtremeWare 7.4 for the module using the download image slot primary command.

3 Configure the module to use the primary image with the use image primary slot command.

4 Reboot the module using the reboot slot command.

NOTE

If you are upgrading multiple modules, skip step 4 until you have upgraded every module, then reboot the switch instead of rebooting each slot.

5 Verify that the correct ExtremeWare is loaded using the show version command.

6 Download the BootROM using the `download bootrom slot` command.

7 Reboot the module using the `reboot slot` command.

NOTE

If you are upgrading multiple modules, skip step 7, upgrade every module, then reboot the switch.

8 Verify the slot is operational using the `show slot <#>` command.

Upgrading PoE Firmware on an Alpine Switch with a PoE Module

If you are using an Alpine switch with a PoE module, upgrade the PoE firmware. A version of PoE firmware is built into ExtremeWare to allow easy replacement if necessary. If the current micro controller firmware becomes corrupted, or requires an upgrade, ExtremeWare logs a message in the syslog prompting for a firmware upgrade.

NOTE

Alpine switches with PoE modules require user intervention using a CLI command to upgrade the PoE firmware. Until this firmware update is completed, the PoE ports are not powered up.

1 Use the following command to download the firmware to the selected slot:

```
download firmware slot <slot_number>
```

2 Verify that the PoE firmware loaded correctly using the `show inline-power stats <slot number>` command.

If the upgrade is not successful, perform the upgrade procedure again.

Upgrading an Alpine 3802 to ExtremeWare 7.4

To upgrade an Alpine 3802 to ExtremeWare 7.4:

1 Upload the configuration to your TFTP server using the `upload configuration` command.

2 Upgrade to BootROM 8.2 using the `download bootrom` command.

3 Reboot the switch using the `reboot` command.

4 If you are using an image prior to ExtremeWare 6.1.8b79, TFTP download ExtremeWare 6.1.8w3.0.1 b79 to the primary image space using the `download image primary` command.

5 Verify that the correct BootROM and ExtremeWare versions are loaded on the switch using the `show switch` and `show version` commands.

6 Answer `y` at the prompt to reboot the switch.

7 TFTP download ExtremeWare 7.0.0b46 to the primary image space using the `download image primary` command.

8 Reboot the switch using the `reboot` command.

9 TFTP download the latest ExtremeWare 7.4 build to the primary image space using the `download image primary` command.

10 Reboot the switch using the `reboot` command.

11 TFTP download the configuration you saved in Step 1, and enter `y` to reboot the switch.

12 Check the log for configuration errors. Manually enter configurations that did not load.

13 Save the new configuration to the primary space.

Do **not** save to the secondary configuration space until you are certain a downgrade to the previous image is not required.

Downgrading “i” Series Switches

Assuming that the previous configuration is in the secondary configuration space and the previous image is in the secondary image space:

1 If you saved an ExtremeWare 6.1 (or earlier) configuration during the upgrade process, configure the switch to use that configuration with the `use configuration secondary` command.

If you did not save an earlier configuration, re-configure the switch or download a configuration at the end of this process.

2 If you did not save the earlier ExtremeWare image in the secondary image space, download the image using the `download image secondary` command.

NOTE

If you downgrade to an ExtremeWare version that does not support software signatures (ExtremeWare 6.2.2b56 or later supports software signatures), you must follow the upgrade procedures in the preceding sections to get back to ExtremeWare 7.3. You cannot switch between primary and secondary images on the switch unless they both support software signatures.

3 Use the image in the secondary image space with the `use image secondary` command.

4 Verify that the above procedures were completed successfully with the `show switch` command.

5 Downgrade to the appropriate BootROM version. The `show version` command displays the BootROM version as “Unknown” when the BootROM is downgraded.

6 Reboot the switch.

NOTE

When downgrading to a previous version of ExtremeWare, ensure that the switch configuration matches the previous version of ExtremeWare or below. Pointing the configuration to a new version of ExtremeWare and using a previous version of ExtremeWare is not supported. You will get a warning message from the system when attempting to do so.

7 If you did not save an ExtremeWare 6.1 (or earlier) configuration during the upgrade process, re-configure the switch or download a configuration.

Upgrading ExtremeWare on Summit 200/300/400 Series Switches Using the CLI

This section describes how to upgrade to ExtremeWare 7.4 on Summit 200/300/400 series switches.

NOTE

Because of the drastic change in the functionality between earlier versions of ExtremeWare 7.4, such as ExtremeWare 6.2e, ExtremeWare 7.1e, and ExtremeWare 6.2a, not all configuration databases are

automatically converted during the initial boot of ExtremeWare 7.4 Failure to download the saved configuration will leave the switch with a minimal default configuration.

Upgrading a Summit 200 to ExtremeWare 7.4

Upgrade a Summit 200 switch running ExtremeWare 6.2e or ExtremeWare 7.1e to ExtremeWare 7.4 as follows:

NOTE

If you are using ExtremeWare 7.1e and stacking is enabled, the stacking functionality has changed drastically in ExtremeWare 7.4. As a result, the CLI commands are not compatible. Refer to the user guide for configuration differences.

NOTE

If you need SSH functionality, first download the non-SSH image as stated above and then download the SSH image. To request SSH code, contact Technical Support.

1. Upload the current configuration to a TFTP server using the `upload configuration` command.
2. Verify the current BootROM is version 5.1. If the BootROM is version 5.1, go to step 5, otherwise download the BootROM: s200_boot51.bin using the `download boot` command and `reboot` command. For example,

   ```
   download boot 10.60.112.254 s200_boot51.bin
   reboot
   ```

3. If you are running a Summit 200 switch with ExtremeWare 6.2e or ExtremeWare 7.1e download ExtremeWare 7.3 image v73e0b43.Fxtr to the primary image space using the `download image primary` command. Otherwise, proceed to step 6.
4. Reboot the switch using the `reboot` command.
5. Download the configuration you saved in step 1. For example:

   ```
   download config 10.60.112.254 saved.cfg
   ```

6. Download the ExtremeWare 7.4 image, v743b5.Fxtr.
7. Save the configuration using the `save configuration` command and reboot the switch using the `reboot` command.
8. The upgrade should not affect the running configuration. If you do not have the appropriate configuration downloaded, reconfigure the switch or download the original configuration saved in step 1. This step is optional.

Upgrading a Summit 300-24 to ExtremeWare 7.4

Upgrade a Summit 300-24 switch to ExtremeWare 7.4 as follows:

1. Upload the current configuration to a TFTP server using the `upload configuration` command.
2. Verify the current BootROM is version 5.1. If the BootROM is version 5.1, go to step 3, otherwise download the BootROM: s200_boot51.bin using the `download boot` command and `reboot` command. For example,

   ```
   download boot 10.60.112.254 s200_boot51.bin
   ```

3 Save the configuration using the `save configuration` command.

4 Download the ExtremeWare 7.4 image, v743b5.Fxtr.

5 Reboot the switch using the `reboot` command.

6 The upgrade should not affect the running configuration. If you do not have the appropriate configuration downloaded, reconfigure the switch or download the original configuration saved in step 1. This step is optional.

Upgrading a Summit 300-48

Upgrade a Summit 300-48 as follows:

1 Verify an ExtremeWare version of at least v62a120b422 is running on the Summit 300-48 using the `show switch` command.

2 If the switch is running the minimum required version, go to step 6.

3 Download v62a120b422.

4 Save the configuration using the `save configuration` command.

5 Reboot the switch using the `reboot` command.

6 Upload the current configuration to a TFTP server.

7 If the switch is running ExtremeWare 7.3 or earlier, download ExtremeWare 7.3 image v73e0b43.Lxtr. Otherwise, proceed to step 9.

8 Save the configuration using the `save configuration` command.

9 Download ExtremeWare 7.4 image v743b5.Lxtr.

10 Reboot the switch using the `reboot` command.

11 Download the configuration you saved in step 6. For example:

```
download config 10.60.112.254 saved.cfg incremental
```

Upgrading a Summit 400-48t to ExtremeWare 7.4

Upgrade a Summit 400-48t to ExtremeWare 7.4 as follows:

1 Upload the current configuration to a TFTP server.

2 Verify the current BootROM is version 5.1. If the BootROM is version 5.1, go to step 3, otherwise download the BootROM: s400_boot51.bin and reboot the switch.

NOTE

If the switch does not accept the BootROM or the image, ensure the 10G2XN module is installed. If the module is installed, remove the module (not just the GBICs but the entire module) from the switch. This module is not hot swappable; power off the switch before removing. The 10 Gig XGM-2XN module is supported in ExtremeWare 7.4 and later. You cannot upgrade or downgrade a Summit switch running an ExtremeWare release earlier the ExtremeWare 7.4.

3 If the switch is running ExtremeWare 7.3 or earlier, download ExtremeWare 7.3 image v73e0b43.Cxtr. Otherwise, proceed to step 5.

4 Save the configuration using the `save configuration` command.

5 Download ExtremeWare 7.4 image v743b5.Cxtr.

6 Reboot the switch using the `reboot` command.

7 Download the configuration you saved in step 1. For example:

```
download config 10.60.112.254 saved.cfg
```

This step is optional.

Upgrading a Summit 400-24 to ExtremeWare 7.4

Upgrade a Summit 400-24 to ExtremeWare 7.4 as follows:

1 Upload the current configuration to a TFTP server.

2 Verify the current BootROM is version 5.1. If the BootROM is version 5.1, go to step 3, otherwise download the BootROM: s405_boot51.bin and reboot the switch.

3 Download ExtremeWare 7.4 image v743b5.Cxtr.

4 Reboot the switch using the `reboot` command.

5 Download the configuration you saved in step 1. For example:

```
download config 10.60.112.254 saved.cfg
```

This step is optional.

Downgrading ExtremeWare

These instructions assume that you followed the upgrade instructions correctly and that the desired previous configuration has been preserved in the secondary configuration space.

1 If the secondary configuration was saved while using a previous image, configure the switch to use the secondary configuration using the `use configuration secondary` command.

2 If there is no stored configuration saved for that version of ExtremeWare, you must either reconfigure, or unconfigure, the configuration file chosen (using the `unconfig switch all` command) or download the correct configuration file to the switch while running the desired image.

3 Use the image in the secondary image space with the `use image secondary` command.

4 Verify that the above procedures were completed successfully with the `show switch` command.

5 Reboot the switch.

6 If you do not have the appropriate configuration downloaded, reconfigure the switch or download the appropriate configuration.

NOTE

When downgrading to a previous version of ExtremeWare, you must ensure that the switch configuration matches that version of ExtremeWare or below. Pointing the configuration to a new version of ExtremeWare and using a previous version of ExtremeWare is not supported.

Upgrading ExtremeWare on Summit Series Switches Using EPICenter 5.0

If you have multiple switches you plan to upgrade to ExtremeWare 7.4, you can use Extreme's EPICenter Management Suite 5.0 software to do a bulk upgrade of these devices. EPICenter's Firmware Manager enables you to do a bulk upgrade of devices of the same type, which greatly speeds and simplifies the upgrade process, and avoids the need to upgrade your switches one by one.

For information on upgrading Summit 200, 300, and 400 series switches to ExtremeWare 7.4 using EPICenter, see the EPICenter 5.0 Service Pack 3 Release Note. For general information on EPICenter 5.0, and on using the EPICenter Firmware Manager, see the EPICenter Reference Guide available on the Extreme Networks website.

3 Supported Limits

This chapter summarizes the supported limits in ExtremeWare 7.4.

NOTE

ExtremeWare 7.4 supports the "i" series platforms, including the BlackDiamond, Alpine, and Summit "i" series switches. In addition, ExtremeWare supports the "e" series platforms, including the Summit 200, Summit 300, and Summit 400 series switches.

This chapter contains the following sections:

Supported Limits for ExtremeWare "i" Series Switches

Table 24 lists the supported limits for the "i" series switches. The contents of this table supersede any values mentioned in the *ExtremeWare 7.4 User Guide.*

Table 24: Supported limits for "i" Series Switches

Metric	Description	Limit
Access List rules	Maximum number of Access Lists (best case).	5120
Access List rules—BlackDiamond 6816	Maximum number of BlackDiamond 6816 Access Lists (best case).	3500
Access List rules—Summit	Maximum number of Access Lists in which all rules utilize all available options (worst case).	255
Access List rules—Alpine	Maximum number of Access Lists in which all rules utilize all available options (worst case).	255
Access List rules—BlackDiamond	Maximum number of Access Lists in which all rules utilize all available options (worst case).	255 per I/O module
Access Profiles	Maximum number of access profiles per switch.	128
Access Profile entries	Maximum number of access profile entries per switch.	256

Table 24: Supported limits for "i" Series Switches (continued)

Metric	Description	Limit
Application Examination rules	Maximum number of Application Examination rules.	1000
Application Examination rules/port	Maximum number of Application Examination rules per port.	60
BGP—Peer Groups	Maximum number of BGP peer groups per switch.	16
BGP—peers	Maximum number of BGP peers per switch.	200
BGP—routes, MSM-3	Maximum number of routes received and contained in the BGP route table (best case).	840,000
BGP—routes, MSM64i	Maximum number of routes received and contained in the BGP route table (best case).	308,000
BGP—routes, Alpine	Maximum number of routes received and contained in the BGP route table (best case).	340,000
BGP—routes, Summit7i	Maximum number of routes received and contained in the BGP route table (best case).	412,000
BGP—routes, Summit48i	Maximum number of routes received and contained in the BGP route table (best case).	102,000
BGP—routes, Summit5i	Maximum number of routes received and contained in the BGP route table (best case).	82,000
BGP—routes, Summit1i	Maximum number of routes received and contained in the BGP route table (best case).	105,000
BGP—NLRI filters	Maximum number of NLRI filters per switch.	127
BGP—NLRI filer add entries	Maximum number of NLRI add entries per switch.	256
BGP—AS-Path filters	Maximum number of AS-Path filters per switch.	127
BGP—AS-Path filter add entries	Maximum number of AS-Path filter add entries per switch.	256
BGP—network statements	Maximum number of network statements per switch.	256
BGP—aggregate addresses	Maximum number of aggregate routes that can be originated per switch.	256
DNS—maximum simultaneous servers	Maximum number of simultaneous domain name servers.	8
DNS—maximum suffixes	Maximum number of simultaneous domain suffixes.	6
EAPS—Domains/switch	Maximum number of EAPS domains.	64
EAPS—Domains/ring	Maximum number of EAPS domains if no switch in the ring is connected to another ring.	64
EAPS—VLAN links	Maximum number of Control or Protected VLANs per EAPS domain.	4093
EAPS—Bridge links	Maximum number of EAPS bridge links per switch.	8192
EAPS—Bridge links	Maximum number of EAPS bridge links on switches with 256MB memory.	8192
EAPS—Bridge links	Maximum number of EAPS bridge links on switches with 128MB memory.	4096
EAPS—Master nodes	Number of Master nodes per EAPS domain.	1
EAPS—Switches	Maximum number of EAPS switches per ring.	No limit

Table 24: Supported limits for "i" Series Switches (continued)

Metric	Description	Limit
EMISTP & PVST+ — maximum domains, Summit	Maximum number of EMISTP and PVST+ domains.	128
EMISTP & PVST+ — maximum domains, Alpine	Maximum number of EMISTP and PVST+ domains.	256
EMISTP & PVST+ — maximum domains, BlackDiamond	Maximum number of EMISTP and PVST+ domains.	512
EMISTP & PVST+ — maximum ports	Maximum number of EMISTP and PVST+ ports.	3840
EMISTP & PVST+ — maximum domains per port, Summit	Maximum number of EMISTP and PVST+ domains that can be configured per port.	128
EMISTP & PVST+ — maximum domains per port, Alpine	Maximum number of EMISTP and PVST+ domains that can be configured per port.	256
EMISTP & PVST+ — maximum domains per port, BlackDiamond	Maximum number of EMISTP and PVST+ domains that can be configured per port.	512
ESRP—maximum domains	Maximum number of ESRP domains for a single switch.	64
ESRP—maximum instances	Maximum number of ESRP supported VLANs for a single switch.	64
ESRP—maximum ESRP groups	Maximum number of ESRP groups within a broadcast domain.	4
ESRP—maximum ESRP groups with bi-directional rate shaping	Maximum number of ESRP groups within a broadcast domain when bi-directional rate shaping is enabled.	3
ESRP—maximum VLANs in a single ESRP domain – Summit, Alpine	Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain.	256 recommended; 3000 maximum
ESRP—number of VLANs in a single ESRP domain, BlackDiamond	Maximum number of VLANs that can be joined to a single ESRP instance through an ESRP domain.	1024 recommended; 3000 maximum
ESRP—Route-track entries, Summit, Alpine, BlackDiamond	Maximum number of routes that can be tracked for each ESRP domain.	4
ESRP—maximum VLAN tracks	Maximum numbers of VLAN tracks per VLAN.	1
FDB—maximum ports for permanent entries	Maximum number of ports supported for permanent FDB entries.	2000
FDB—maximum L2/L3 entries – BlackDiamond, Summit5i, Summit7i, Alpine 3804, Alpine 3808	Maximum number of MAC addresses/IP host routes for the MSM64i, Summit5i, Summit7i, Alpine 3804, and Alpine 3808.	262,144
FDB—maximum L2/L3 entries – Summit1i, Summit48i, Summit48si, Alpine 3802	Maximum number of MAC addresses/IP host routes for the Summit1i, Summit48i, Summit48si, and Alpine 3802.	131,072
Flow Redirection—maximum redirection rules	Maximum number of rules that can point to the same or separate groups of web cache servers.	64 (8 servers is the maximum)
Flow Redirection—maximum enumeration mode entries	Maximum number of active entries for enumeration mode rules. For example, one /16 rule can take all of the available entries.	32,764
Flow Redirection—maximum subnet mode entries	Maximum number of active entries for subnet mode rules. Each mask can have 1 entry.	64
IP ARP entries	Maximum number of IP ARP entries.	20,480

Table 24: Supported limits for “i” Series Switches (continued)

Metric	Description	Limit
IP ARP Static entries	Maximum number of permanent IP static ARP entries supported.	512
IP ARP Static Proxy entries	Maximum number of permanent IP ARP proxy entries.	512
IP Route Sharing Entries (ECMP)—static or OSPF	Maximum number of static or OSPF routes used in route sharing calculations.	12
IP Route Sharing Entries (ECMP)—IS-IS	Maximum number of IS-IS routes used in route sharing calculations.	8
IP Router interfaces	Maximum number of VLANs performing IP routing - excludes SubVLANs.	512
IP Static Routes	Maximum number of permanent IP routes.	1024
IPX Static Routes and Services (RIP and SAP)	Maximum number of static IPX RIP route and IPX SAP entries.	64 for each
IPX dynamic routes and services	Maximum recommended number of dynamically learned IPX RIP routes and SAP entries.	2000 for each
IPX Router interfaces	Maximum number of IPX router interfaces.	256
IPX Access control lists	Maximum number of Access Lists in which all rules utilize all available options.	worst case: 255
IS-IS—maximum routing interfaces	Maximum IS-IS routing interfaces.	255
IS-IS—maximum routes	Maximum IS-IS routes.	25,000
IS-IS—maximum adjacencies	Maximum IS-IS adjacencies per routing interface.	64
IS-IS—maximum domain summary addresses	Maximum IS-IS domain summary addresses.	32
IS-IS—maximum redistributed routes, regular metric	Maximum IS-IS redistributed routes using the regular metric.	20,000
IS-IS—maximum redistributed routes, wide metric	Maximum IS-IS redistributed routes using the wide metric.	30,000
IS-IS—maximum redistributed routes, both metrics	Maximum IS-IS redistributed routes using both metrics.	10,000
Jumbo Frame size	Maximum size supported for Jumbo frames, including the CRC.	9216
Logged Messages	Maximum number of messages logged locally on the system.	20,000
MAC-based VLANs—MAC addresses	Maximum number of MAC addresses that can be downloaded to the switch when using MAC-based VLANs.	7000
MAC-based security	Maximum number of MAC-based security policies.	1024
Mirroring—mirrored ports	Maximum number of ports that can be mirrored to the mirror port.	8
Mirroring—number of VLANs	Maximum number of VLANs that can be mirrored to the mirror port.	8
NAT—maximum connections	Maximum number of simultaneous connections per switch.	256,000
NAT—maximum rules	Maximum number of rules per switch.	2048
NAT—maximum VLANs	Maximum number of inside or outside VLANs per switch.	The switch’s limit

Table 24: Supported limits for "i" Series Switches (continued)

Metric	Description	Limit
NetFlow—Filters	Maximum number of NetFlow filters in a switch.	128
NetFlow—Groups	Maximum number of NetFlow groups.	32
NetFlow—Hosts	Maximum number of NetFlow hosts.	8/group
Network Login—Maximum clients	Maximum number of Network Login clients per switch.	1024
Network Login—802.1x	Maximum recommended Session-Timeout value returned by RADIUS server.	7200 seconds
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF external routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of external routes contained in an OSPF LSDB of an internal router in the OSPF domain.	Summit 71—130,000 Alpine—115,000 BlackDiamond—100,000
OSPF intra-area routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of intra-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain.	Summit 71—11,500 Alpine—10,000 BlackDiamond—9,000
OSPF inter-area routes—BlackDiamond, Summit7i, Alpine	Recommended maximum number of inter-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain.	16,000
OSPF external routes—Summit1i, Summit5i, Summit48i, Summit48si	Recommended maximum number of external routes contained in an OSPF LSDB of an internal router in the OSPF domain.	27,000
OSPF intra-area routes—Summit1i, Summit5i, Summit48i, Summit48si	Recommended maximum number of intra-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain.	2000
OSPF inter-area routes—Summit1i, Summit5i, Summit48i, Summit48si	Recommended maximum number of inter-area routes contained in an OSPF LSDB of an ABR router in the OSPF domain.	8000
OSPF routers in a single area	Recommended maximum number of routers in a single OSPF area.	200
OSPF interfaces on a single router	Recommended maximum number of OSPF routed interfaces on a switch.	384
OSPF virtual links	Maximum number of OSPF virtual links supported.	32
OSPF adjacencies—Summit1i, Summit5i, Summit48i, Summit48si	Maximum number of OSPF adjacencies on a switch with 128 MB memory.	150
OSPF adjacencies—Summit7i, Alpine, BlackDiamond	Maximum number of OSPF adjacencies on a switch with 256 MB memory.	225
RIP-learned routes	Maximum number of RIP routes supported without aggregation.	8000
RIP interfaces on a single router	Recommended maximum number of RIP routed interfaces on a switch.	384
Route Maps	Maximum number of route maps supported on a switch.	128
Route Map Entries	Maximum number of route map entries supported on a switch.	256
Route Map Statements	Maximum number of route map statements supported on a switch.	512
SLB—maximum number of simultaneous sessions	For Transparent and Translational and GoGo modes respectively.	500,000/500,000/ unlimited

Table 24: Supported limits for “i” Series Switches (continued)

Metric	Description	Limit
SLB—maximum number of VIPs	For Transparent and Translational and GoGo modes respectively.	1000/1000/unlimited
SLB—maximum number of Pools	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—maximum number of Nodes per Pool	For Transparent and Translational (does not apply to GoGo mode)	256/256
SLB—maximum number of physical servers per group	Applies to GoGo mode only; a group shares any number of common VIPs.	8
SNMP—Trap receivers	Maximum number of SNMP trap receiver stations supported.	16
SNMPv3—Users	Maximum number of SNMPv3 users.	32
SNMPv3—Groups	Maximum number of SNMPv3 groups.	64
SNMPv3—Accesses	Maximum number of SNMPv3 accesses.	128
SNMPv3—MIB-views	Maximum number of SNMPv3 MIB-views.	128
SNMPv3—Communities	Maximum number of SNMPv3 communities.	64
SNMPv3—Target addresses	Maximum number of SNMPv3 target addresses.	16
SNMPv3—Target parameters	Maximum number of SNMPv3 target parameters.	16
SNMPv3—Notifications	Maximum number of SNMPv3 notifications.	8
SNMPv3—Filter profiles	Maximum number of SNMPv3 notify filter profiles.	16
SNMPv3—Filters	Maximum number of SNMPv3 notify filters.	400
Spanning Tree—maximum STPDs, Summit	Maximum number of Spanning Tree Domains.	128
Spanning Tree—maximum STPDs, Alpine	Maximum number of Spanning Tree Domains.	256
Spanning Tree—maximum STPDs, BlackDiamond	Maximum number of Spanning Tree Domains.	512
Spanning Tree—minimum STPDs	Minimum number of Spanning Tree Domains.	1
Spanning Tree—802.1d domains	Maximum number of 802.1d domains per port.	1
Spanning Tree—minimum number of ports	Minimum number of ports that can participate in a single Spanning Tree Domain.	1
Spanning Tree—minimum number of domains/port	Minimum number of Spanning Tree Domains that can be configured per port.	1 for default VLAN, 0 for others
Spanning Tree—Spanning Tree modes	Maximum number of Spanning Tree modes per switch.	2 (dot1d and dot1w)
SSH2—number of sessions	Maximum number of simultaneous SSH2 sessions.	8
Standard Multinetting—Maximum secondary IP addresses per switch	Maximum secondary IP addresses that can be configured per switch.	64
Standard Multinetting—Maximum secondary IP addresses per VLAN	Maximum secondary IP addresses that can be configured per VLAN.	64
Static MAC FDB entries—Summit, Alpine, BlackDiamond	Maximum number of permanent MAC entries configured into the FDB.	4096
Super-VLAN—number of ports & sub-VLANs	Maximum number of ports and sub-VLANs associated with each super-VLAN.	2550

Table 24: Supported limits for “i” Series Switches (continued)

Metric	Description	Limit
Syslog servers	Maximum number of simultaneous syslog servers that are supported.	4
Telnet—number of sessions	Maximum number of simultaneous Telnet sessions.	8
Trusted MAC entries	Maximum number of simultaneous trusted MAC entries.	48
UDP profiles	Number of profiles that can be created for UDP forwarding.	10
UDP profile entries	Number of entries within a single UDP profile.	16
VLANs—Summit, Alpine	Includes all VLANs plus sub VLANs, super VLANs, etc.	4095
VLANs—BlackDiamond 6816 fully populated	Includes all VLANs plus sub VLANs, super VLANs, etc.	681
VLANs—BlackDiamond 6816 with up to 7 I/O modules	Includes all VLANs plus sub VLANs, super VLANs, etc.	1776
VLANs—BlackDiamond	Includes all VLANs plus sub VLANs, super VLANs, etc.	4095
VLANs—maximum active protocol-sensitive filters	The number of simultaneously active protocol filters in the “i” series or Summit 400 switch.	15
VRRP—maximum VRIDs	Maximum number of unique VRID numbers per switch.	4
VRRP—maximum VRIDs with bi-directional rate shaping	Maximum number of unique VRID numbers per switch when bi-directional rate shaping is enabled.	3
VRRP—maximum VLANs/switch	Maximum number of VLANs per switch.	64
VRRP—maximum VRIDs/VLAN	Maximum number of VRIDs per VLAN.	4
VRRP—maximum ping tracks	Maximum number of ping tracks per VLAN.	4
VRRP—maximum iproute tracks	Maximum number of iproute tracks per VLAN.	4
VRRP—maximum VLAN tracks	Maximum number of VLAN tracks per VLAN.	1

Supported Limits for ExtremeWare “e” Series Switches

Table 25 summarizes tested metrics for a variety of features in the ExtremeWare 7.4 “e” series switches. These limits may change but represent the current status. The contents of this table supersede any values mentioned in the *Summit 400 Series Switch Installation and User Guide*.

Table 25: Supported limits for “e” Series Switches

Metric	Description	Limit
Access Lists/Rate Limits	Maximum number of access list rules, including rate limit rules	Summit 200-24—990 Summit 200-48—1740 Summit 300-24—990 Summit 300-48—1980 Summit 400-24—1536 Summit 400-48—5800
Access Profiles	Used by SNMP, Telnet, SSH2, and Routing Access Policies	128

Table 25: Supported limits for “e” Series Switches

Metric	Description	Limit
Access Profile entries	Used by SNMP, Telnet, SSH2, and Routing Access Policies	256
EAPS—Domains/switch	Maximum number of EAPS domains.	4
EAPS—Domains/ring	Maximum number of EAPS domains if no switch in the ring is connected to another ring.	4
EAPS—VLAN links	Recommended maximum number of Control or Protected VLANs per switch.	128
EAPS—Master nodes	Number of Master nodes per EAPS domain.	1
EAPS—Switches	Maximum number of EAPS switches per ring.	No limit
FDB—Maximum multicast entries	Maximum number of multicast entries for the switch.	Summit 400—255 Summit 200 and Summit 300—252
FDB—Maximum number of L2 entries	Maximum number of MAC addresses.	Summit 400—16,000 Summit 200 and Summit 300—8000
FDB—Maximum number of L3 entries	Maximum number of IP addresses.	Summit 200 and Summit 300—2000 Summit 400-24—2000 Summit 400-48—4000
IP Router interfaces	Maximum number of VLANs performing IP routing.	Summit 400-24—128 Summit 400-48—512 Summit 200—32 Summit 300—32
IP Route Sharing Entries	Maximum number of IP routes used in route sharing calculations. This includes static routes and OSPF ECMP.	8
IP Static ARP entries	Maximum number of permanent IP static ARP entries supported.	512
IP Static Routes	Maximum number of permanent IP routes.	1024
Load Sharing groups	Maximum number of groups.	Summit 200—6 Summit 300-24—6 Summit 300-48—5 Summit 400—25
Load Sharing ports/group	Maximum number of ports per group.	8
Mirroring—Mirrored ports	Maximum number of ports that can be mirrored to the mirror port.	8 (however, more than 3 may affect performance)
Multicast Groups	Maximum number of multicast groups.	Summit 200—252 Summit 300—252 Summit 400-24—127 Summit 400-48—255
Network Login—802.1x	Maximum recommended session timeout value returned by RADIUS server.	7200
Network Login—Maximum Clients	Network login maximum clients.	1024
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF intra-area routes	Recommended maximum number of intra-area routes contained in an OSPF LSDB.	5000
OSPF inter-area routes	Recommended maximum number of inter-area routes contained in an OSPF LSDB.	5000

Table 25: Supported limits for “e” Series Switches

Metric	Description	Limit
OSPF external type 1 or 2 routes	Recommended maximum number of external type 1 or 2 routes contained in an OSPF LSDB.	100,000
OSPF routers in a single area	Recommended maximum number of routers in a single OSPF area.	40
OSPF interfaces on a single router	Maximum number of OSPF routed interfaces on a switch.	2
OSPF interfaces, passive	Maximum number of passive OSPF interfaces.	512
OSPF virtual links	Maximum number of OSPF virtual links supported.	2
OSPF adjacencies	Maximum number of OSPF adjacencies on a switch.	4
Rate Limits	Maximum number of rate limit rules.	3024
Packet buffer—10/100/1000 port	Size of the packet buffer on each 10/100/1000 port.	80 KB
RIP-learned routes	Maximum number of RIP routes supported without aggregation.	8000
RIP interfaces on a single router	Recommended maximum number of RIP routed interfaces on a switch.	32
SSH2—number of sessions	Maximum number of simultaneous SSH2 sessions.	8
SNMP—Trap receivers	Maximum number of SNMP trap receiver stations supported.	16
SNMPv3—Users	Maximum number of SNMPv3 users.	32
SNMPv3—Groups	Maximum number of SNMPv3 groups.	64
SNMPv3—Accesses	Maximum number of SNMPv3 accesses.	128
SNMPv3—MIB-views	Maximum number of SNMPv3 MIB-views.	128
SNMPv3—Communities	Maximum number of SNMPv3 communities.	64
SNMPv3—Target addresses	Maximum number of SNMPv3 target addresses.	16
SNMPv3—Target parameters	Maximum number of SNMPv3 target parameters.	16
SNMPv3—Notifications	Maximum number of SNMPv3 notifications.	8
SNMPv3—Filter profiles	Maximum number of SNMPv3 notify filter profiles.	16
SNMPv3—Filters	Maximum number of SNMPv3 notify filters.	400
Syslog servers	Maximum number of simultaneous syslog servers that are supported.	4
Spanning Tree—Maximum STPDs	Maximum number of Spanning Tree Domains.	Same as the number of available physical ports on the switch
Spanning Tree—Maximum number of ports	Maximum number of ports that can participate in a single Spanning Tree Domain.	Same as the number of available physical ports on the switch
Static IP ARP Proxy entries	Maximum number of permanent IP ARP proxy entries.	512
Static MAC FDB entries	Maximum number of permanent MAC entries configured into the FDB.	128
Telnet—number of sessions	Maximum number of simultaneous Telnet sessions.	8
UDP profiles	Number of profiles that can be created for UDP forwarding.	10

Table 25: Supported limits for “e” Series Switches

Metric	Description	Limit
UDP profile entries	Number of entries within a single UDP profile.	16
VLANs	Maximum number of VLANs (includes all VLANs).	Summit 400—4094 Summit 200—255 Summit 300—255

Stacking Limits for Power over Ethernet

When creating a stack of Summit 200 and Summit 300-24 switches, the maximum number of Power over Ethernet (PoE) capable switches to be used is three. When stacking Summit 400 switches, up to eight PoE capable switches can be stacked. The time it takes to make all PoE ports operational increases with the number of PoE capable switches in the stack.

Table 26: Supported limits for stacking Summit Series switches

Metric	Description	Stacking Limits
Access Lists/Rate Limits	Maximum number of access list rules, including rate limit rules	It is the sum of all individual switch limitations in the stack.
Access Profiles	Used by SNMP, Telnet, SSH2, and Routing Access Policies	128
Access Profile entries	Used by SNMP, Telnet, SSH2, and Routing Access Policies	256
EAPS—Domains/switch	Maximum number of EAPS domains.	4
EAPS—Domains/ring	Maximum number of EAPS domains if no switch in the ring is connected to another ring.	4
EAPS—VLAN links	Recommended maximum number of Control or Protected VLANs per switch.	128
EAPS—Master nodes	Number of Master nodes per EAPS domain.	1
EAPS—Switches	Maximum number of EAPS switches per ring.	No limit
FDB—Maximum multicast entries	Maximum number of multicast entries for the switch.	Master switch limitations apply to the entire stack. If the master is: Summit 400—255 Summit 200 and Summit 300—252
FDB—Maximum number of L2 entries	Maximum number of MAC addresses.	Master switch limitations apply to the entire stack. If the master is Summit 400—16,000 Summit 200 and Summit 300—8000

Table 26: Supported limits for stacking Summit Series switches

Metric	Description	Stacking Limits
FDB—Maximum number of L3 entries	Maximum number of IP addresses.	Master switch limitations apply to the entire stack. If the master is: Summit 200 and Summit 300—2000 Summit 400-24—2000 Summit 400-48—4000
IP Router interfaces	Maximum number of VLANs performing IP routing.	Master switch limitations apply to the entire stack. If the master is: Summit 400-24—256 Summit 400-48—512 Summit 200—32 Summit 300—32
IP Route Sharing Entries	Maximum number of IP routes used in route sharing calculations. This includes static routes and OSPF ECMP.	8
IP Static ARP entries	Maximum number of permanent IP static ARP entries supported.	512
IP Static Routes	Maximum number of permanent IP routes.	1024
Load Sharing groups	Maximum number of groups.	Master switch limitations apply to the entire stack. If the master is: Summit 200—6 Summit 300-24—6 Summit 400—25
Load Sharing ports/group	Maximum number of ports per group.	8
Mirroring—Mirrored ports	Maximum number of ports that can be mirrored to the mirror port.	8 (however, more than 3 may affect performance).
Multicast Groups	Maximum number of multicast groups.	Master switch limitations apply to the entire stack. If the master is Summit 200—252 Summit 300—252 Summit 400-24—127 Summit 400-48—255
Network Login—802.1x	Maximum recommended session timeout value returned by RADIUS server.	7200
Network Login—Maximum Clients	Network login maximum clients.	1024
OSPF areas	As an ABR, how many OSPF areas are supported within the same switch.	8
OSPF intra-area routes	Recommended maximum number of intra-area routes contained in an OSPF LSDB.	5000
OSPF inter-area routes	Recommended maximum number of inter-area routes contained in an OSPF LSDB.	5000
OSPF external type 1 or 2 routes	Recommended maximum number of external type 1 or 2 routes contained in an OSPF LSDB.	100,000

Table 26: Supported limits for stacking Summit Series switches

Metric	Description	Stacking Limits
OSPF routers in a single area	Recommended maximum number of routers in a single OSPF area.	40
OSPF interfaces on a single router	Maximum number of OSPF routed interfaces on a switch.	2
OSPF interfaces, passive	Maximum number of passive OSPF interfaces.	512
OSPF virtual links	Maximum number of OSPF virtual links supported.	2
OSPF adjacencies	Maximum number of OSPF adjacencies on a switch.	4
Rate Limits	Maximum number of rate limit rules.	3024
Packet buffer—10/100/1000 port	Size of the packet buffer on each 10/100/1000 port.	80 KB
RIP-learned routes	Maximum number of RIP routes supported without aggregation.	8000
RIP interfaces on a single router	Recommended maximum number of RIP routed interfaces on a switch.	32
SSH2—number of sessions	Maximum number of simultaneous SSH2 sessions.	8
SNMP—Trap receivers	Maximum number of SNMP trap receiver stations supported.	16
SNMPv3—Users	Maximum number of SNMPv3 users.	32
SNMPv3—Groups	Maximum number of SNMPv3 groups.	64
SNMPv3—Accesses	Maximum number of SNMPv3 accesses.	128
SNMPv3—MIB-views	Maximum number of SNMPv3 MIB-views.	128
SNMPv3—Communities	Maximum number of SNMPv3 communities.	64
SNMPv3—Target addresses	Maximum number of SNMPv3 target addresses.	16
SNMPv3—Target parameters	Maximum number of SNMPv3 target parameters.	16
SNMPv3—Notifications	Maximum number of SNMPv3 notifications.	8
SNMPv3—Filter profiles	Maximum number of SNMPv3 notify filter profiles.	16
SNMPv3—Filters	Maximum number of SNMPv3 notify filters.	400
Syslog servers	Maximum number of simultaneous syslog servers that are supported.	4
Spanning Tree—Maximum STPDs	Maximum number of Spanning Tree Domains.	Same as the number of available physical ports on the stack.
Spanning Tree—Maximum number of ports	Maximum number of ports that can participate in a single Spanning Tree Domain.	Same as the number of available physical ports on the stack.
Static IP ARP Proxy entries	Maximum number of permanent IP ARP proxy entries.	512
Static MAC FDB entries	Maximum number of permanent MAC entries configured into the FDB.	128
Telnet—number of sessions	Maximum number of simultaneous Telnet sessions.	8

Table 26: Supported limits for stacking Summit Series switches

Metric	Description	Stacking Limits
UDP profiles	Number of profiles that can be created for UDP forwarding.	10
UDP profile entries	Number of entries within a single UDP profile.	16
VLANs	Maximum number of VLANs (includes all VLANs).	Master switch limitations apply to the entire stack. If the master is: Summit 400—4094 Summit 200—255 Summit 300—255

4 Clarifications, Known Behaviors, and Resolved Issues

This chapter describes items needing further clarification, behaviors that might not be intuitive, and issues that have been resolved since the last release. Numbers in parentheses are for internal reference and can be ignored.

This chapter contains the following sections:

Clarifications and Known Behaviors

Following are the clarifications and known behaviors in ExtremeWare 7.4. For changes made in previous releases, see the release notes specific to the release.

General

Downgrading from ExtremeWare 7.4 to ExtremeWare 7.3 or Earlier Causes a Failure

Downgrading from ExtremeWare 7.4 to ExtremeWare 7.3 or earlier causes the software to fail.

Workaround.

1. Upload the ExtremeWare 7.4 configuration.
2. Run the `unconfigure switch all` command.
3. Downgrade the switch to ExtremeWare 7.3 or earlier.
4. Download the configuration.

(PD3-45120099)

Port Sharing Between G24T and G8X I/O Modules is not Working Correctly

Cross module port sharing involving a G24T and G8X I/O module is not working correctly and generates the following error message:

```
* BD6808:21 # en shar 7:1 g 7:1,8:1
ERROR: Ports 7:1 and 8:1 are running at different speeds.
```

You can only load share on links operating at same speed.

(PD3-37325552)

Some APs Reboot in Heavy Traffic and High RF Interference

A switch with 20 plus APs and a high level of RF interference may experience up to three AP reboots in a 24-hour period (PD3-36148261).

Enabling HTTP on a Non-SSH ExtremeWare 7.4 Image

In ExtremeWare 7.3, the CLI command syntax used to enable HTTP is `enable web http` even when upgrading a non-ssh image. In ExtremeWare 7.4, the `enable web` command is use with the option `http/https`. This command option is only available with the ssh image. Therefore, when upgrading an ExtremeWare 7.3 non-ssh configuration to an ExtremeWare 7.4 non-ssh configuration, the `enable web http` command will fail.

```
# enable web http
Syntax error at token http
Next possible completions:
<cr> access-profile
```

Upgrading the Switch to ExtremeWare 7.4 from ExtremeWare 7.2 or Earlier

When the BlackDiamond, Alpine, and Summit switches are upgraded from ExtremeWare 7.2 or earlier to ExtremeWare 7.4, you may see the following error messages. These error messages are harmless as these commands are not supported on the management VLAN in ExtremeWare 7.4.

```
- configure vlan "Mgmt" priority 0
ERROR: Cannot modify 802.1P Priority for the Mgmt Vlan
configure vlan "Mgmt" qosprofile "QP1"
ERROR: vlan "Mgmt" cannot be configured
configure vlan Mgmt qosprofile ingress none
WARNING: This command only applies to the G16X3 and G24T3 I/O modules.
```

(PD3-1303781)

Load Sharing Group Cannot be Rate Shaped with Loopback Port

You cannot configure a load sharing group for rate shaping with a loopback port, nor can you tag a rate shaped port, even though the CLI is allowing you to do so (PD2-243742672).

CPU DoS Protect and ACL Precedence

If you configure the CPU DoS protect feature with a filter precedence of x, you cannot create an access list with a precedence of x, x+1, or x+2. All other values are acceptable.

If you configure an access list with a precedence of x, you cannot configure the CPU DoS protect feature with a filter precedence of x, x-1 or x-2. All other values are acceptable (PD2-129163428).

Alpine

EPICenter/SNMP Does not Show Port Display String

When configuring a port string using an Alpine switch and viewing the port information from EPICenter, the configured port string is not shown in the port information (PD3-40520509).

BlackDiamond 6800

BlackDiamond Switch Generates L2 Known Unicast Traffic

A BlackDiamond switch is generating L2 known unicast traffic after disabling and enabling a slot (PD3-40044661).

Summit 200, Summit 300-48, and Summit 400 Switches

AP Not Coming Up in Remote Connect

The AP is not coming up in remote connect after switching from direct connect.

Workaround. Create a separate VLAN for the discovery switch for the AP upgrade (direct connect).

(PD3-46430702)

Loopback Detect Does Not Work on ExtremeWare 7.4e.1b5

On a Summit 300-48 switch running ExtremeWare 7.4e.1b5, if you connect loopback on a specific port and then enable loopback detect, loopback is detected and the port is brought down after 3 or 4 hours. The port is then bought up and down continuously (PD3-39424321).

Opnext ER XENPAKs Generate an Error Message

Opnext ER XENPAKs used in a Summit-400-48t switch generates the following error message and causes the switch port to not come up:

```
04/05/2005 14:15:20.38 <Erro:PORT> Xenpak on port 49 detected, unable to read Oui,
possible mdio read error.
```

(PD3-38955593)

Bi-Directional Rate Shaping

Changing the Configuration of a Loopback Port

If you change the configuration (speed, duplex setting, etc.) of a loopback port, you must either save the configuration and reboot the switch, or delete the port from the VLAN and add it back (PD2-128242637, PD2-127582534).

Bridging

Deleting Member VLANs Flushes FDB Entries

Deleting a member VLAN flushes all FDB entries in the translation and member VLANs (PD3-24824553).

CLI

Configurations are Corrupted When Switch is Rebooted

Configurations are corrupted when the switch is rebooted after performing a change in the local configuration and downloading a new configuration (PD2-232396030).

Control Protocols

VRRP Backup Does Not Flood Packets

On "e" series switches, VRRP backup does not flood packets destined for the virtual MAC address(PD3-42286365).

EAPS Link Down PDU Not Sent from the Transit Switch After Rebooting

Create two EAPS rings between three switches and reboot the transit switch. After rebooting, disable the slot that connects the two transit switches. The link-down PDU is not received on the master switch from the transit switch. The link-down PDU is received from the other transit switch (PD3-40658231).

Diagnostics

Upgrading from ExtremeWare 6.2.2 to ExtremeWare7.x Enables FDB Scan

When upgrading from ExtremeWare 6.2.2 to ExtremeWare 7.x, after you reboot the switch and issue the `show configuration detail` command the following FDB scan message is displayed:

```
configure fdb-scan period 255
enable fdb-scan
```

Workaround. When upgrading from ExtremeWare 6.22 to ExtremeWare 7.x, issue the following CLI commands when you bootup the switch:

```
disable fdb-scan
unconfigure fdb-scan period
```

(PD3-24841137)

EAPS

Flushing Selective FDB Entries is not Working Properly on an EAPS Domain

Selective flushing of FDB entries belonging to a protected VLAN is not working correctly. Instead, the switch flushes all FDB entries, including those for non-protected VLANs (PD3-37488841).

ESRP

Rate-shaped ESRP Slave Interface Loses Some of the ESRP Hello Packets

A rate-shaped ESRP slave interface loses some of the ESRP hello packets from the master and flips between the slave and pre-master state when the election parameters suit the slave to win the ESRP election (PD3-26798641).

PoE

Default PoE Algorithm on All Ports is max-class-operator

The default setting for all ports on a Summit 300-48 switch is `max-class operator` and `advertised class`. The maximum class operator is by default set for 15.4 W, or Class 3 only. The default setting should be `advertised class`.

Workaround. To set all ports to be `advertised-class` the procedure is as follows.

1. Issue the `disable inline-power` command.
2. Issue the `config inline-power violation-precedence advertise-class ports all` command.

(PD3-26067537)

RADIUS

Authentication With Secondary Radius Server Fails After Switch Reboot

Assuming both the primary and the secondary RADIUS servers are configured, when you unconfigure the primary RADIUS server, the failover to the secondary RADIUS server happens correctly. The wireless client is able to be authenticated using a secondary RADIUS server, but after the switch reboots, authentication is not successful with the secondary RADIUS server (PD3-36227684).

Routing

Exported Static Route in ISIS is Advertised After Removing the VLAN and Static Route

If a VLAN is removed prior to removing a static route, the exported static route is not removed, even after removing the static route configuration.

Workaround. Remove the static route before deleting the VLAN with the gateway IP address.

(PD3-31673591)

SNMP

MIB Table Becomes Empty When Adding Policy Rules through EPICenter

When adding multiple IP policy rules through EPICenter's Policy Manager, frequently the MIB table will become empty or partially cleared (only some of the rules will remain), even though no error message has occurred, and the policy rules are still in place on the switch. When this happens it is no longer possible to create policies on the switch through EPICenter (PD3-36028540).

lldpLocSysDesc Returns Hex Value (Unreadable Characters)

When querying lldpLocSysDesca a hex value is returned (unreadable characters). Since this object type is Display String, this object should return a readable string value (PD3-35723021).

lldpStatsRemTablesLastChangeTime Displays Wrong Value

When you query the object lldpStatsRemTablesLastChangeTime through SNMP the wrong value is displayed (PD3-35723085).

LLDP Enabled Port in LldpLocManAddrTable Object

One entry should be created for each LLDP enabled port in the LldpLocManAddrTable object. When the MIB table is queried, it returns only the management address of the first enabled LLDP port (PD3-35774621).

CLI Allows Creation of Duplicate Trap Receivers

The CLI `configure snmp add trapreceiver` command allows you to configure duplicate trap receivers with the same port, community string, and trap group without generating an error message (PD2-118394805).

SNMP Response Time from the Switch is Slow

SNMP response time from the switch is slow when the number of APs configured for the switch is more than seven. EPICenter polling may result in a SNMP failure since the default setting for SNMP is 5s timeout and 1 retry.

Workaround. Increase the timeout value in SNMP Client Tool. Suggested values for more than seven APs: timeout: 7 seconds; retry = 2.

(PD3-36087851)

Switch Does Not Log a Message When Using SNMP to Change a Configuration

Currently the switch will not log a message when the configuration is changed using SNMP (PD3-35398661).

Extreme Real Time Statistics Does Not Work When There are 24+ Ports

When Network Management tool EPICenter tries to get real time statistics on an Extreme device that has more than 24 ports, it sometimes fails (PD3-14524212, PD3-15975950).

Stacking

Bootup Time

A full stack consisting of 8 Summit 200 or Summit 300-24 switches amy take slightly over two minutes to bootup. However, a full stack of Summit 400 switches would take just under two minutes on the average to bootup.

Traffic Grouping Based on Access Lists, DSCP Across Units Not Working Properly

Traffic grouping based on access-lists across units on a Summit 200-48, or across slots in a stack of Summit 200 series switches is not supported (PD3-35723040).

Task Utilization is High During a CPU DoS Attack

When CPU-DoS protection is enabled in Stacking mode and a Dos attack is attempted on the switch high task utilization is observed (PD3-27794280).

Configuring the Mirrored-to Port

Once you configure the mirrored-to port to be either tagged or untagged, if you change it from tagged to untagged, or from untagged to tagged, the change will only take affect after a reboot (PD3-29054741).

VLAN Tagged 2 Cannot be Used When Stacking is Enabled

If stacking is enabled on the switch, the switch will not allow you to create a user VLAN with a tag of 2 (PD3-30253861).

CLI Commands Executed from Pseudo TTY Sessions

Running CLI commands executed from pseudo-TTY sessions results in excessive and incomplete output (PD3-23616276, PD3-25226542).

Moving from a Stack Image to a Non-stack Image

When moving from a stack image to a non-stack image, run the `disable stacking` command or chose the `nonstack conf` option (PD3-29013801).

Wrong Number of Ports Displayed in Default VLAN

The default VLAN shows the incorrect number of active ports after all ports are deleted from the VLAN if the following procedure is followed:

1. Save the configuration using the ExtremeWare 7.4 image.
2. Reboot the switch and save the configuration using the ExtremeWare 7.3 image.
3. Reboot the switch to the ExtremeWare 7.4 image using the saved ExtremeWare 7.3 configuration.

4 If all ports are deleted from the default VLAN, the incorrect number of active ports is shown.

(PD3-28261405)

Frames Being Received After Setting MAC Limit to Zero for Port

In a stack of two Summit switches, create a VLAN and add some ports. Set the MAC limit to zero on one of the ports. If you send frames from that port to the other port, the receiving port should receive one frame when in fact it is receiving multiple frames (PD3-25226331).

Able to Receive Frames Even After Port is Locked for Learning

After creating a VLAN and adding ports from the master and backup switches, once you lock MAC address learning, all frames should be discarded but some multiple frames, not all, are received (PD3-24903111).

Ninth Switch Introduced in a Stack Does Not Become the Stand-alone Master

When connecting a switch to a stack of eight switches through the stack port and enabling stacking in the added switch, the added switch, or ninth switch, stays in the "Discovery State" and does not become a stand-alone master (PD3-24239271, PD3-24272096, and PD3-24272111).

bcmRX Drops Messages When Adding or Deleting a VLAN with Traffic

When adding or deleting a VLAN with traffic on a stacking DUT, the console is flooded with the following error message:

```
[bcmRx] ATP RX Dropping non-ready rx trans...
```

(PD3-26514621)

Stacking Supports Up to a Maximum of 8 Switches

In ExtremeWare 7.4, the current stacking implementation supports up to a maximum of 8 switches in a stack. However, under certain configuration scenarios, the maximum number supported per switch may be less than 8. Refer to the *ExtremeWare 7.4 User Guide* for more information (PD3-26601290).

Mix Mode Stacking is not Supported

Mixed mode stacking, that is, stacking between Summit 200/300/400 series switches, is not supported in this release (PD3-25989591).

Downloading a Configuration to a Stack

After downloading a configuration to a stack, all slots must be operational before attempting to save the configuration (PD3-27126942).

Wireless

Special Characters Accepted in WEP Plaintext Key

While configuring the WEP Plaintext key, the following characters are accepted in the CLI and are also stored as part of the key:

* - (hyphen)
* _ (underscore)
* . (dot)

For example, `eg.con sec open64wep wep key add 0 plaintext a-_..` would be an accepted key.

The following character is accepted in the CLI but is not stored as part of the key:

* # (hash)

For example, `eg.con sec open64wep wep key add 0 plaintext a-_..############` is accepted by the switch, but is seen as identical to the previous example.

The following characters are rejected in the CLI:

* ~'@$%^&*()+={[}]|\:;"'<,>?/

For example, `eg.# con sec open64wep wep key add 0 plaintext abcd'` generates a syntax error at the `'` character.

(PD3-36227502)

show wireless ports detail Output Changes to Incorrect Value after Wireless Port IP is Modified

When you change the IP address of a wireless port that is online, the "Src IP in logs" in the `show wireless ports <port> detail` command output displays a wireless Gateway IP instead of a modified wireless port IP (PD3-26541091).

WPA-PSK Client Unable to Connect if Passphrase is More than 12 Characters

If you set a WPA-PSK passphrase using more than 12 characters, the wireless client cannot connect successfully (PD3-35947702).

SNMP Error Messages are Generated When Wireless Port is Reset

When you reset a wireless port that is online, the following SNMP error messages are logged:

```
03/14/2005 17:26:01.47 <Erro:WLANSYST> <WLAN> Port 1 SNMP failed to parse the packet
with 7a198
03/14/2005 17:26:01.47 <Info:WLANSYST> <WLAN> Port 1 Wireless Port Down
03/14/2005 17:26:01.10 <Info:SYST> 10.255.52.7 admin: reset wireless ports 1
```

(PD3-36028901)

show wireless ports detail Output Shows Incorrect BootStrap/BootLoader Version

The `show wireless ports <port> detail` command shows the incorrect bootstrap and bootloader version for the AP when the AP is running an older bootrom version (1.5.2).

```
# show wireless ports 2 detail
...
Hardware Version: 01010001
Software Version: v7.3.1
Bootstrap Version:        v0.0.0
Primary Bootloader Ver:        v64.240.254 (Booted)
Secondary Bootloader Ver:        v212.240.254
```

On a Summit 300-48, the APs bootstrap and bootloader software are upgraded automatically. On a Summit 400-24p, Summit 300-24, and Alpine switches the upgrade facility is not available. Therefore, the issue of incorrect version display is only seen on Summit 400-24p, Summit 300-24, and Alpine switches (PD3-35947955).

Stacking and UAA Functionality

UAA functionality is stated to be available on a master slot of a stack in the *ExtremeWare 7.4 User Guide*. This is incorrect. UAA is not supported on any stacking. This will be corrected in future updates of the *ExtremeWare 7.4 User Guide* (PD3-36334122).

Wireless Network Login ISP Mode Shown in the Incorrect State

When the switch is configured for ISP mode and a wireless client is successfully authenticated using Network Login, the `show wireless ports interface clients detail` command correctly shows the wireless client to be in the FORWARD state. However, if the client logs out and is re-authenticated, the `show wireless ports interface clients detail` command shows the wireless client to be in the ASSOC state (PD3-36087675).

Wireless Network Login User May be able to Access Network Resources

When an authenticated wireless Network Login client disconnects using the client software, instead of using the logout popup window, the Network Login session is sometimes not cleared in the switch. As a result, when the client reconnects to the AP, the client can access network resources even though the client is in the unauthenticated state (PD3-35950208).

show wireless ports detail Output Shows Incorrect Software Version

The `show wireless ports <port> detail` command shows the incorrect software version for the AP. The software version should read v 7.4.1.

```
# show wireless ports 1 : 14 det
...
Hardware Version:         01010001
Software Version:         v7.3.1
```

(PD3-35950133)

Wireless Client Cannot Move to a Permanent VLAN

A wireless client cannot move to a permanent VLAN if ISP mode is changed to Campus mode on the same port.

Workaround. When changing ISP mode to Campus mode configuration, instead of assigning Campus mode configuration to the same wireless port, assign Campus mode to a different wireless port.

(PD3-36087982)

Changing Switch Time Resets APs Time Incorrectly

Changing the switch time backwards resets the time on the AP incorrectly. When you run the `show wireless ports` and `show wireless ports interface clients detail` commands the output shows the `Last state change` field incorrectly.

Workaround. Reset the wireless port so that the AP can get the correct time.

(PD3-30472539)

Wireless Client Sees Wrong Log Message

Wireless clients on A radio show 11930 hours of logged on time when the `show wireless ports 1:X interface 1 clients` command is executed.

```
00:20:A6:4C:FE:C1 1:44:1 FORWARD   WEP128   DOT1X      11930:25:41
```

This is usually a cosmetic problem. The logged on time shows the correct value after the next RADIUS timer refresh (PD3-28788118).

TCP/IP Connection is Lost if Internal DHCP is Enabled

The TCP/IP connection between the switch and the AP is lost if internal DHCP is enabled and wireless Network Login is not configured on the wireless port (PD3-35311601).

Wireless Network Login Displays Incorrect User at Log Out

When a wireless Network Login user logs out using the logout window, the log message displays the wrong user name (PD3-33544205).

IAPP Does Not Support WPA

IAPP roaming works with the following authentication methods:

- Open WEP
- Shared WEP
- Open MacRadius
- Shared MacRadius
- dot1x

IAPP is not supported for WPA (PD3-29602669).

Logout Window Moves to “Cannot Find Server”

The logout pop-up window moves to the "cannot find server" state after x minutes in Network Login (PD3-28788428).

A300 Cannot Boot

The A300 cannot boot if the wireless management VLAN is not configured (PD3-28462210, PD3-23854771).

Some IAPP Debug Messages Are Not Logged

If you configure debug-trace for wireless ports to debug-level 5 and set the syslogd priority to debug, when you roam from one AP to another AP, the `show log` command does not display all of the IAPP debug messages, whereas the `show wireless ports x:y log` command displays all IAPP debug messages correctly (PD3-28462355, PD3-6273069).

HTTP/Vista Not Supported

HTTP/Vista is not supported for UAA and stacking switches (PD3-34980791, PD3-28462001, PD3-25236381).

Do Not Enable AP_Scan on More than Two Interfaces at a Time

If you enable the AP scan on more than two interfaces simultaneously, the scan will run for a few minutes but once you issue the `show wireless ap-scan results` command, the switch reboots (PD3-28764622, PD3-3868131).

Issues Resolved in ExtremeWare 7.4.3b5

The following issues were resolved in ExtremeWare 7.4.3b5. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.4 includes all fixes up to and including ExtremeWare 6.2.2b156, 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, and ExtremeWare 7.3e.3b4. For information on those fixes, see the release notes for those releases.

General

When ports 49 and 50 are connected to the same Summit48si switch, the link now comes up after disconnecting and reconnecting the ports (PD3-29219826).

The tConsole task no longer fails when rebooting a Summit 300-48 with an Edge License (PD3-50850031, PD3-47315999).

False watchdog failures for an MSM3 are no longer reported when the chassis is powered up (PD3-42138961).

The tAgentX task no longer crashes in a BlackDiamond switch with the Exception Program Counter (EPC) pointing to ip_to_port_lookup (PD3-47646881).

When transmitting 64 Kbps fixed packets at 100 Mbps through a hub to two Summit 48i switches running ESRP, the secondary Summit 48i no longer slows down during packet transmission (PD3-47310391, PD3-48946469).

A TCP connection no longer goes into the TCP close/wait state after receiving TCP packets with the following bit set: SYN,FIN,PUSH,URGENT (PD3-45723439).

BlackDiamond

Stand-alone BlackDiamond 6808 switches with an F48Ti module installed no longer experience high port utilization (PD3-42179804).

Summit

On a Summit 300-48 switch, the tRootTask no longer crashes, causing the switch to reboot in a loop (PD3-55381783).

On a Summit 200 switch, the internal setting for the gigabit ports (25, 26) signal detect level is now correct (PD3-51650617.

Redundant ports on a Summit 200 switch now work normally if the redundant port is a fiber port (PD3-48957841).

The watchdog timer no longer expires after configuring an ACL rule on a Summit 200-48 switch (PD3-36947251).

The gigabit port I/O module voltage has been reset to 2.5 V on Summit 200 switches (PD3-52558235, PD3-48564913).

Summit 300-48 switches no longer fail after rebooting when wireless is not enabled (PD3-48946414).

Running the `show switch` command on a Summit 300-48 switch with an empty (default) configuration no longer generates the following message:

```
:<Erro:KERN> NV:readImageTime: failed reading memory from FLASH (2)
```

(PD3-36934571)

ACL

Access-profiles with subnet entries set to `deny` now work even though the major network is set to `permit` (PD3-22951023).

Bridging

Source MAC refresh is no longer causing multicast traffic to be out of order (PD3-55235712).

The tBGTask no longer crashes when processing IGMP snoop data input (PD3-53419191).

EAPS links are no longer reported as down when the primary link in a load-share configuration goes down (PD3-51289451).

NetBIOS protocol based VLANs now recognize LLC f0f1 packets (PD3-45191631).

CLI

T3 ports can now be added to multiple VLANs without generating an incorrect error message (PD2-149180105).

The switch no longer hangs when displaying the `configure lacp keep-alive 3` command when executing the `show configuration` command (PD3-29936386).

The `enable/disable web https` command is no longer available on BlackDiamond switches running image v732b3.Sxtr (PD3-43162530).

Diagnostics

Enabling transceiver diagnostics and running extended diagnostics on MSM-B no longer triggers a false alarm (PD2-244409185).

EAPS

After rebooting, the VPST state now resets to forwarding on the EAPS shared port (PD3-53419213).

When the EAPS ring consists of T1 ports, EAPS transition no longer results in the wrong active port counter in the protected VLAN (PD3-48719481).

ESRP

The ESRP active port count, numActivePorts, no longer reverts to 0 when one of the ports in the ESRP VLAN is configured as an ESRP host attached port (PD3-55234183).

When a Summit 400 is used as an ESRP Aware switch, link flap no longer causes an ESRP dual master (PD3-49967751).

ESRP now follows the actual physical link up count when performing an ESRP failover (PD3-48009461).

Multicast

On Summit 400 switches, you can now delete CPU bits added to IP multicast FDB entries (PD3-52400175).

Summit 200-48 switches now forward multicast traffic from port 49 to port 50 when IP multicast traffic ages out (PD3-52399639, PD3-52399621).

On Summit 200, Summit 300, and Summit 400 switches, the first multicast packet received after source learning and clearing the multicast FDB is no longer forwarded twice (PD3-43009727, PD3-48913901).

Network Login

In web-based Network Login, when clients log out, the client MAC address no longer remains in the FDB table (PD3-45622071).

Lock-learning is no longer allowed on ports that have Network Login enabled (PD3-38469981).

RADIUS

With RADIUS enabled, the watchdog timer no longer expires while the tRadProxy task is running on a BlackDiamond 6808 (PD3-49979291).

Routing

Packets are now forwarded with the correct MAC address when being forwarded through the MPLS I/O module (PD3-50648341).

The Summit 200 no longer reboots during large IP FDB synchronizations (PD3-48552431).

If PIM snooping is disabled on a VLAN and the switch is running the `show pim` command, the VLAN no longer generates an assertion failure (PD3-35581552).

Security

Memory allocated for processing SNMP traps received by the switch from a wireless Access Point is freed correctly (PD3-48498531).

SNMP

Community string configuration using Vista is now successfully applied (PD3-791401).

When performing an SNMP Get, `extremeFdbMacFdbMacAddress.<x>.<x>` now works properly on a Summit 400 switch (PD3-41789041).

After disabling SNMP traps for port-up-down on a management port, the trap is correctly disabled (PD3-28675172).

Stacking

In a stacking configuration, the master switch no longer fails during periods of heavy traffic (PD3-47762081).

The `show stacking port rxerrors` command no longer displays CRC errors when unicast/multicast packets are flooded (PD3-46257741, PD3-43284151).

When load sharing is configured across slots, if the load sharing master port goes down, multicast traffic is now sent over the load sharing secondary port. However, when a new multicast entry is created with the configured load shared primary port down, the traffic does not egress by way of the new operational load shared primary port. Nevertheless, for the existing entries, the traffic will be switched correctly (PD3-35672901).

When a link up/link down event occurs on a load shared trunk port that is spanned across the primary and secondary slots, it no longer causes the system to fail (PD3-52601801).

In a load sharing configuration on a Summit 400 switch, IP multicast entries are created in the stack and traffic goes out on the load shared operating master port (PD3-35940395).

A stack of Summit 400 switches no longer experiences a higher level of multicast packet loss for nodes attached to the master switch with IGMP snooping disabled (PD3-50708471).

The `save configuration secondary` command no longer saves the configuration as `primary` instead of `secondary` (PD3-40395629).

Interfaces now link ports at speeds faster than 10 Mbps (PD3-35852851).

Vista

Accessing a stack using Vista over an SSH connection and selecting Configuration > Ports no longer reboots the switch (PD3-42871441).

ExtremeWare Vista now displays the correct IP ARP entries (PD3-41602680).

VRRP

Edge series switches no longer forward IP packets destined for the VRRP MAC in the VRRP backup state (PD3-48957937).

Wireless

After upgrading from ExtremeWare 7.3 to ExtremeWare 7.4 on a Summit 300-48 switch, users are no longer authenticated through the local database if the RADIUS server is configured and RADIUS is enabled (PD3-29875281).

Issues Resolved in ExtremeWare 7.4.2b6

The following issues were resolved in ExtremeWare 7.4.2b6. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.4 includes all fixes up to and including ExtremeWare 6.2.2b156, ExtremeWare 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.3b4, and ExtremeWare 7.3e.3b4. For information on those fixes, see the release notes for those releases.

General

The collision counter in the `show ports txerrors` command stops incrementing after the port has been disconnected (PD3-41400271, PD3-35472391).

Downloading configurations no longer causes the fdb-scan period to revert back to the default value regardless of the configured saved value (PD3-26785011).

The AP TFTP client can now communicate with the Linux TFTP server (PD3-44441481).

L3 entries can now be added without causing the following unit error message:

```
Could not add L3 entry for unit 3-10.13.254.116 at 0xaff<-6:Table full>
```

(PD3-42027996, PD3-18120101)

The `save configuration` command no longer fails when saving large configurations (PD3-40441343).

Current TCP/IP implementations are no longer vulnerable to ICMP attacks (PD3-29757217, PD3-41714816).

All unknown unicast or broadcast packets are now sent to the same ingress port when MSM-B is removed or inserted (PD2-244409172).

The MSM-failover link-down now brings down the link on the remote side of the switch, not just the fiber ports (PD2-246448109, PD2-246448118).

In software redundant gigabyte ports on a Summit 48si, the link state is now correctly changed when removing and reinserting redundant links with the master link in the inactive state (PD3-25896001, PD3-3891361).

Links no longer flap on neighbor switches when smart redundancy is disabled on a Summit 48si switch (PD3-14292583).

BlackDiamond

The G12sxi and F96ti I/O module backplane links are now reconnecting to MSM-A when MSM-B disabled (PD3-24444382).

The following error message no longer continually displays on all ports on the I/O modules when an MSM fails over on a BlackDiamond 6808 switch:

```
<Errno:SYST> getNMCIntPort(): wrong port 6 for card 1
<Errno:SYST> backplaneHealthCheck(): Failed to get destination card information
frrorm card 0 port 4.
```

(PD3-858003)

Running the `synchronize` command on a BlackDiamond 6816 running ExtremeWare 7.3.2b3 will not cause the MSM-3 to hang (PD3-41063122).

Performing a hitless failover with an F96Ti I/O module no longer causes packet loss (PD3-26774062).

Summit 200, Summit 300-24, and Summit 400 Switches

The manufact_init( ) routine now clears the odometer on Summit 200, Summit 300, and Summit 400 switches (PD3-39606977).

On a Summit 200 switch, when BOOTP is enabled on the VLAN, packets with 21st octet 0x08 are bridged (PD3-36164581).

Processing a large number of slow-path packets at one time no longer locks the stackTask, causing stacking control packets to drop and stacking to stop functioning properly (PD3-41175669, PD3-41909449).

Network Login clients are no longer logged out every 5 minutes on Summit 200, Summit 300, and Summit 400 platforms (PD3-40219306).

Runtime diagnostics no longer fail the CPU loopback test when traffic is being sent on the gigabit ports (PD3-38371321).

If you connect an Extreme Networks-approved cable in the port-to-port loopback configuration and run the diagnostics tests on stacking ports, the cable test no longer fails (PD3-36542560).

You will no longer experience packet drop with the XGM-2xn module on a Summit 400-48 switch (PD3-36478661).

Bridging

When the `nobroadcast` option is enabled on a port, broadcast packets are now forwarded to other ports (PD3-42325794).

Switches transmitting traffic with full IP FDB entries do not periodically reboot because of watchdog timer expiry (PD3-39558371).

Transmitting packets between MSMs no longer causes packet loss or an increase in packet count (PD3-32365081).

Control Protocols

When disabling and enabling ELSM on a port, the following error message is no longer displayed:

```
hoCliEvent: Command does not support Hitless Failover
```

(PD2-182478105)

Diagnostics

Watchdog state now automatically re-enables if diagnostics are run consecutively on two or more I/O modules (PD3-36934629).

Extended diagnostics now run on the Summit5i SX switch (PD3-28859001).

Flow Redirection

Enabling or disabling flow redirection no longer causes a task crash or MSM failover (PD3-37002531, PD3-37895848).

EAPS

If an MSM failover occurs, the EAPS shared port no longer goes into an idle state (PD3-32427358).

EAPS link down PDUs are now received on the master switch when sent from the transit switch (PD3-40658231).

The switch no longer flushes all FDB entries, including those for non-protected VLANs, in an EAPS domain (PD3-41415471, PD3-37488841).

Multicast

IP multicast cache entries are no longer deleted and recreated every 2 hours as long as there is traffic using the multicast cache entry (PD3-42221350, PD3-28376251).

SNMP

After configuring port mirroring and issuing the `snmpset -v1 -c private <ipaddress of switch> ifStatckStatus.52.48 i destroy` command, the switch no longer stops responding to SNMP requests (PD3-32427101).

Spanning Tree Protocol

The PVST BPDUs are now flooded through the switch when s0 (dot1d) is enabled (PD3-37431601, PD3-35301361, PD3-29658822).

Stacking

LLDP now runs on the secondary ports of a load-sharing group (PD3-35886082).

You can ping remote IP devices in the default VLAN even when the ports are spread across slots (PD3-38469181).

Wireless

Memory is now allocated correctly in the AP running a WPA2 security profile when clients are continuously logging in and logging out of the switch (PD3-39390951).

Non-DFS channels are no longer included on the Radar interference list; only supported DFS channels are included (PD3-38764191).

Issues Resolved in ExtremeWare 7.4.1b5

The following issues were resolved in ExtremeWare 7.4.1b5. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.4 includes all fixes up to and including ExtremeWare 6.2.2b156, 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.2b3, and ExtremeWare 7.3e.2b4. For information on those fixes, see the release notes for those releases.

General

When a static MAC address is configured across a load share group, the packets arriving with a static MAC as the source are no longer dropped by the load share group (PD3-22738261).

Upgrading from ExtremeWare 6.2.2 to ExtremeWare 7.2.0 now correctly reads stored non-volatile configurations for FDB scan and transceiver diagnostics (PD3-26362998, PD3-26774271).

The following error message is no longer displayed if you have only one PSU installed in a Summit 300-48:

```
05/04/2005 22:19:01.17 <Crit:KERN> PSU-B Not Present
05/04/2005 22:19:01.17 <Crit:KERN> PSU A OK
05/04/2005 22:19:01.14 <Info:SYST> PSU-A not installed.
```

(PD3-33299927)

BlackDiamond

When using a BlackDiamond 6816, inserting a second power supply no longer interrupts I/O module behavior (PD3-24997371).

On a BlackDiamond switch, STP ports are no longer shown as loopback ports (loopback flag "L" enabled) during a STP topology change (PD3-24938998).

Bridging

The switch no longer accepts load sharing ports that are set at different speeds (PD3-26857032).

Spanning Tree Protocol

All ports of a default VLAN are now shown as part of the default STP domain s0 on an Alpine switch (PD3-27096541).

Stacking

When eight Summit 200 switches are connected, stack formation no longer fails (PD3-26798611).

Clearing a console session on a slave slot now functions properly (PD3-26482929).

Layer 2 forwarding is no longer affected if a slot with a load share link is rebooted (PD3-27134464).

On a Summit 200-48t switch, load sharing traffic is no longer sent on the master port only (PD3-21484658).

In a two switch stack, the switch no longer stops responding when issuing any of the following CLI commands:

- `enable stp`
- `disable stp`
- `enable vrrp`
- `disable vrrp`
- `enable eaps`

(PD3-25926111)

If a stack reboots while multicast streams are on, after the formation of the stack, tStackTask and tNetTask no longer show high CPU utilization (PD3-28633931).

If a stack reboots while the multicast streams are on, it no longer takes a considerable amount of time to form the protocol adjacencies (PIM, RIP, and OSPF) (PD3-28632362).

On the slave switch, the link status no longer shows as active even after disabling the port (PD3-28831248).

The number of active ports displayed after a save and reboot is now correct (PD3-26925793).

Stacking port information in ifTable is now accurate (PD3-26629639).

The display for interface type for stack port is now correct in the interfaceEntry MIB table (PD3-26654772).

The link speed for the stack port displays in the interfaceEntry MIB table (PD3-26654788).

Change in the link status trap is no longer missed (PD3-26752662).

Summit switches that are used as a stack master switch no longer cause traffic to stop forwarding and the switch to reboot after a watchdog timer reset (PD3-26784871).

SNMP

When exercising the route table in the FDB MIB with dot1dTpFdbTable enabled, high CPU utilization messages are no longer displayed in the syslog (PD2-102926801).

Switching

Server load balancing traffic is no longer being forwarded to servers that are down (PD3-25374396).

Vista

Clicking on the access-list page no longer generates an error message (PD3-24863521.)

VRRP

Tracking a VLAN no longer generates an error message (PD3-24087800).

IP FDB learning no longer takes too much time causing the VRRP state to continuously flip (PD3-28476981).

Wireless

The `show log` command no longer generates SNMP error messages on a version upgrade from ExtremeWare v73e1b6-br-UAA1-4-14.Lxtr to ExtremeWare v740b42.Lxtr (PD3-30138621).

Issues Resolved in ExtremeWare 7.4.0b42

The following issues were resolved in ExtremeWare 7.4.0b42. Numbers in parentheses are for internal use and can be ignored. ExtremeWare 7.4 includes all fixes up to and including ExtremeWare 6.2.2b156, 7.1.1b16, ExtremeWare 7.2.0b37, ExtremeWare 7.3.2b3, and ExtremeWare 7.3e.2b4. For information on those fixes, see the release notes for those releases.

General

Downloading a configuration and rebooting the switch no longer generates DOS related error messages (PD3-29650001).

The following message is no longer displayed after a system reboot:

```
CRITICAL ERROR: Backplane EEPROM has invalid MAC Address. System halted.
```

This would occur when both MSM A and MSM B were trying to read the backplane EEPROM without first determining which MSM was master/slave (PD3-5605327).

Bi-directional Rate Shaping

When disabling and re-enabling trunking, the ports no longer lose their configured aggregate-bandwidth values (PD3-24426807).

BlackDiamond

Hot-removal of the slave MSM is less likely to lock up the master MSM. This was caused by a timing problem when the MSM tried to access a module that had been removed from the switch (PD3-8661915).

With BootROM 8.1, using the `reboot slot [msm-a | msm-b]` command via a direct console connection to a slave MSM locks up the MSM. To avoid this, use the command through a Telnet session or a connection to the master MSM. If the MSM is locked up, reboot it using the `reboot slot [msm-a | msm-b] hard` command (PD2-225327825).

The system now makes a best effort attempt to recover from I/O module front panel ports going down on insertion of the slave MSM (PD2-236217801).

When you run the show version command, the system no longer reports that all I/O modules are missing in the switch. The software can now access the EEPROM of the slave and I/O modules. (PD2-238647301).

Running extended diagnostics on a BlackDiamond 6816 slave or switching MSM no longer occasionally causes the MSM to get stuck in the `diag` or `booted` state (PD2-231288735).

Alpine

Running the `disable slot` command on an Alpine switch no longer has the potential to cause checksum errors and/or the loss of Quake buffers. (PD2-247185701).

Diagnostics

Running the `reboot slot msm` command on a BlackDiamond 6816 switching MSM no longer causes the slave MSM to reboot instead (PD2-236446804).

The MSM-B, MSM-C, and MSM-D no longer get stuck in the "booted" state after running diagnostics on a BlackDiamond 6816 (PD2-231288735).

Security

After a client is authenticated using Network Login/dot1x, VSA information is not ignored and VLAN movement is allowed after authentication (PD3-29771291, PD3-26522751).

Wireless

During a configuration upload, the following commands now contain client-history information:

```
enable wireless ports <portlist> interface [1|2] client-history
configure wireless ports <portlist> interface  [1|2] client-history size <number>
configure wireless ports <portlist> interface [1|2] client-history timeout <seconds>
show configuration {detail}
show configuration wireless {detail}
```

(PD3-20720464, PD3-18166701)

In ExtremeWare 7.4, a wireless security profile with Network Auth as WPA and Encryption as WEP (64 or 128), is no longer supported. During configuration upgrade from ExtremeWare 7.3 to ExtremeWare 7.4, the WPA-WEP security profile (if configured) will be converted to a dot1x-WEP security profile (PD3-26773851).